Цитаты номера

В последнее время активность РФ в части *интернационализации* управления интернетом в части изменения полномочий ICANN резко усилилась. В преддверии Всемирной конференции по международной электросвязи МСЭ в Дубаи 3–14 декабря 2012 г. ожидается, что в рамках группы БРИКС будут сформулированы новые предложения по изменению баланса сил по основным вопросам управления интернетом с возможной передачей большей части соответствующих полномочий Международному союзу электросвязи. При этом такие страны, как Бразилия, Индия и Южная Африка, готовы к некоему промежуточному, компромиссному варианту, при котором противостояние между ICANN и МСЭ может быть разрешено в пользу вновь создаваемой международной организации или специализированного учреждения ООН.

В свое время перед теми, кто стоял у истоков интернета, была поставлена такая задача: создать сеть, которая сможет выдержать даже массированный ядерный удар. Во время природных бедствий, таких как цунами в Японии в 2011 г. или землетрясение на Гаити в 2010 г., интернет оказался едва ли не единственным работающим средством связи. Вся остальная инфраструктура, за исключением спутниковой связи, вышла из строя, а интернет продолжал функционировать, и люди могли связаться друг с другом. Поэтому если архитектура интернета спроектирована и сбалансирована должным образом, то никакого *рубильника смерти* в Сети быть не может.

Великобритания не считает Будапештскую конвенцию *О киберпреступности* совершенным документом. В этой области есть еще над чем работать, и именно с этой точки зрения мы будем рассматривать все новые инициативы. При этом между Россией и Западом существует не так уж много противоречий относительно того, как добиться желаемого результата в области борьбы с киберпреступностью на международном уровне. Однако любое возможное соглашение с Россией по вопросам кибербезопасности должно содержать акцент на совершенствование системы международного сотрудничества по борьбе с киберпреступностью и обеспечивать соответствующую среду для поддержания стабильности всего киберпространства.

Сегодня России необходима прежде всего *Стратегия кибербезопасности* верхнего, национального уровня, в которую будет входить список из конечного и конкретного списка задач, которые необходимо решать, а также сроки, к которым их надо решить. Нужны не общие слова, а конкретика. И исполнителями этой стратегии должны быть не только государственные органы и органы власти, но и все задействованные и заинтересованные стороны, включая граждан в частном качестве. Что особенно важно, в обеспечении кибербезопасности должен принимать активное участие бизнес.

С учетом взаимосвязи элементов глобальной информационной сети, кибервойна затронет в той или иной мере ее всю. По этой причине предотвращение кибервойн является задачей каждого государства, включая Россию и ее западных партнеров. Однако сегодня международные усилия по формированию режима безопасности киберпространства явно недостаточны. Наращивание США ударного киберпотенциала вкупе с нежеланием обсуждать юридически обязывающие международно-правовые акты тормозит выход мирового сообщества из латентного состояния *войны всех против всех* по Томасу Гоббсу, перенесенной в киберпространство. Государства мира предпочитают готовиться к кибервойнам, а не пытаться исключить их возможность.

Михаил Якушев

Маркус Куммер

Джейми Сондерс

Андрей Колесников

Олег Демидов

ИНДЕКС БЕЗОПАСНОСТИ № 1 (104), Том 19

ВЕСНА 2013

Журнал ПИР-Центра

Российский журнал о международной безопасности

SECURITY INDEX

ИНДЕКС БЕЗОПАСНОСТИ

№ 1 (104) 2013

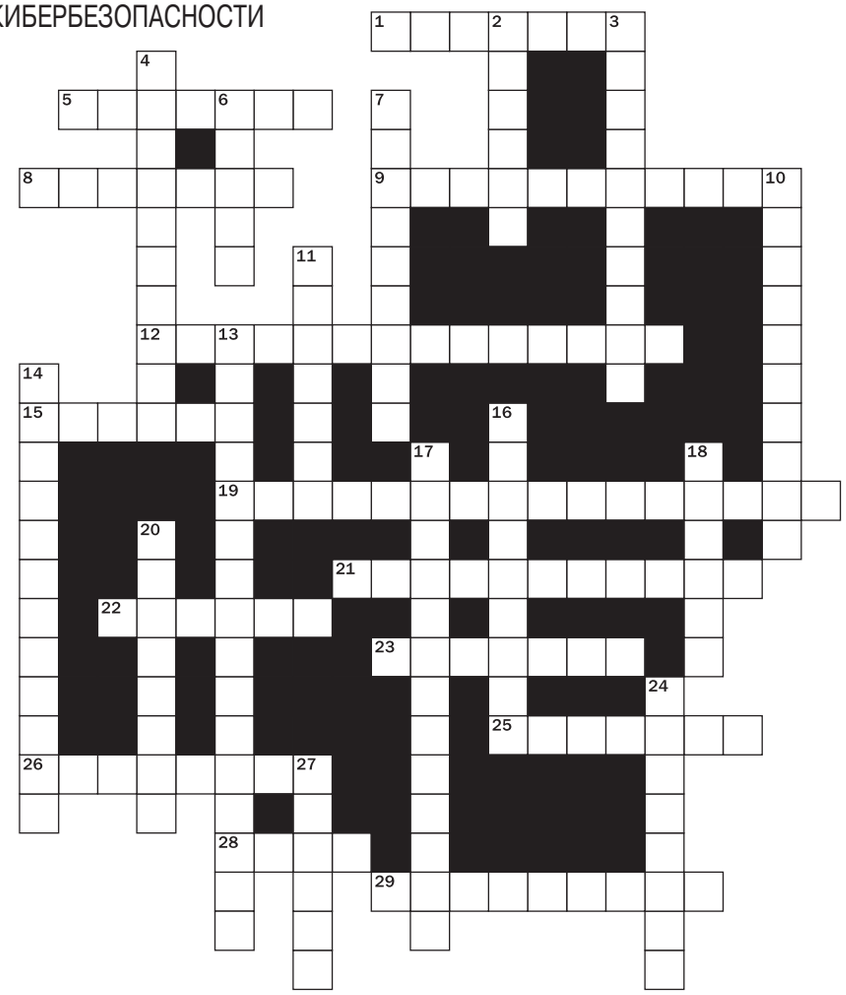
Журнал ПИР-Центра политических исследований России

ТЕМА НОМЕРА:

ГЛОБАЛЬНАЯ БЕЗОПАСНОСТЬ В ЦИФРОВУЮ ЭПОХУ

Олег Демидов ✦ Елена Зиновьева ✦ Галия Ибрагимова
Андрей Колесников ✦ Крис Палларис ✦ Максим Симоненко
Джейми Сондерс ✦ Хамадун Туре ✦ Михаил Якушев

29 СЛОВ О КИБЕРБЕЗОПАСНОСТИ



ПО ГОРИЗОНТАЛИ: 1. Социальная сеть, которая была бы третьим в мире после Индии и Китая государством по численности населения, если бы ее пользователи получили ее гражданство. 5. Востребованный онлайн-инструмент сетевой дипломатии и новое глобальное сетевое СМИ. 8. Основное устройство доступа в глобальную сеть, оттеснившее на второе место персональный компьютер в начале 2010-х гг. 9. Наука, без которой было бы невозможно развитие компьютерных сетей и информационных систем. 12. Техническая процедура проверки подлинности пользователя в компьютерной сети. 15. Упрощенное название сервисов на основе распределенных вычислений, получающих сегодня широкое распространение в ИТ-секторе. 19. Особенность интернета, которая делает принципиально невозможным управление им по принципу иерархии. 21. Прозрачная нить, ставшая одним из ключевых элементов физической инфраструктуры широкополосных телекоммуникационных систем, включая Интернет. 22. Город в Иране, место расположения обогатительного объекта, на котором в результате компьютерной атаки было выведено из строя промышленное оборудование. 23. Средства, позволяющие осуществлять фильтрацию сетевых пакетов и давшие Китаю возможность построить свою «Великую стену» в Интернете. 25. Вид хакерской атаки, заключающийся в использовании чужого IP-адреса с целью обмана системы безопасности. 26. Потомок сети, созданной в конце 1960-х гг. в США в качестве надежного канала поддержания связи и обмена информацией на случай ядерной войны с СССР. 28. Большинство входящих сообщений в вашем почтовом ящике. 29. Процедура, позволяющая устанавливать авторов кибератак и возлагать на них ответственность за совершенные действия.

ПО ВЕРТИКАЛИ: 2. Когда он падает, работа в организации встает. 3. Глава одной из крупнейших в мире антивирусных лабораторий и автор идеи о создании киберМАГАТЭ. 4. Агрессивный акт в отношении компьютерных систем и содержащейся в них информации, осуществляемый при помощи программных средств. 6. Вредоносная программа, неспособная распространяться в компьютерных сетях самостоятельно, а только с человеческой помощью. 7. Форма общественного и политического протеста в Интернете путем причинения ущерба компьютерным сетям и ресурсам при отсутствии корыстных либо криминальных целей. 10. Особенность общения пользователей в Интернете, позволяющая им избегать раскрытия своей личности. 11. Информационное наполнение веб-сайтов и сетевых ресурсов. 13. Фундаментальное свойство Интернета, не позволяющее контролировать его отдельным национальным государствам. 14. Основное назначение современной глобальной сети и значительной части существующих информационных технологий. 16. Программное средство для борьбы с любыми разновидностями вредоносного кода. 17. Фундаментальный принцип Интернета, предусматривающий равенство любых видов передаваемой информации и гарантирующий равные права на доступ в интернет для всех пользователей. 18. Сеть из зараженных вредоносным кодом компьютеров, часто используемая для DDoS-атак без ведома владельцев пораженных машин. 20. Компьютерный червь, признанный многими экспертами первым настоящим кибероружием. 24. Дыра в Сети, куда утекают и откуда попадают в открытый доступ секреты спецслужб, дипломатов и военных различных государств мира. 27. Объем информации, передаваемый по сети за определенный период времени.

Разгаданный кроссворд направляйте заместителю главного редактора И. Мироновой по электронной почте editor@pircenter.org с пометкой «Security Puzzles». Трое читателей, первыми приславшие в редакцию правильные ответы, получат бесплатную подписку на журнал до конца 2013 г. (3 номера). Имена победителей и правильные ответы будут опубликованы в следующем номере.

Научно-практический журнал ПИР-Центра (Центра политических исследований России)

Non multa, sed multum

Выходит четыре раза в год на русском и английском языках

ИНДЕКС БЕЗОПАСНОСТИ

№ 1 (104), Том 19
Весна 2013

Российский журнал о международной безопасности

SECURITY INDEX

Издается с ноября 1994 г. (с 1994 по 2006 г. выходил под названием «Ядерный Контроль»)

ISSN 1992-9242

Москва • Женева • Монтерей

ИНДЕКС БЕЗОПАСНОСТИ

Издается с ноября 1994 г. В период с 1994 до 2006 г. выходил под названием *Ядерный Контроль*.
Выходит четыре раза в год на русском и английском языках.
Зарегистрирован в Федеральной службе по надзору за соблюдением законодательства в сфере массовых коммуникаций и культурного наследия.
Свидетельство о регистрации ПИ № ФС 77-26 089 от 9 ноября 2006 г.

№ 1 (104), Том 19
Весна 2013

Контактная информация

Адрес для писем:
Россия, 119019, Москва, а/я 147
Редакция *Индекса Безопасности*
Телефон редакции:
+7 (495) 987-1915 (многоканальный)
Факс: +7 (495) 987-1914

Интернет-представительство: http://si.pircenter.org

Подписка:

- по России и СНГ: Роспечать, индекс 80666 (см. с. 212)
- по России и СНГ: Пресса России, индекс 10337, http://www.pressa-rf.ru/cat/
- по России: Интер-Почта, индекс 11893, http://www.interpochta.ru/
- по всему миру: ООО *Триалог*, http://pircenter.org/club, tralogue@pircenter.org
- по всему миру: East View Information Services, http://www.eastview.com/
- международное издание: Routledge (Taylor & Francis Group), http://www.tandf.co.uk/journals

Редакционная политика

- Материалы *Индекса Безопасности* не могут быть воспроизведены полностью либо частично в печатном, электронном или ином виде без письменного разрешения Издателя
- Публикуемые материалы, суждения и выводы могут не совпадать с точкой зрения редакции и являются исключительно взглядами авторов
- Выпуск осуществлен благодаря поддержке Министерства иностранных дел и по делам Содружества Великобритании.

Тираж (российское и международное издания) 2000 экз. **Подписано в печать** 25 октября 2012 г.
Отпечатано в ООО «Центр полиграфических услуг «Радуга» по заказу ПИР-ПРЕСС

PIRPRESS

СОДЕРЖАНИЕ

спондента журнала *Индекс Безопасности* отвечает директор и главный консультантом компании *i-intelligence*.

Ключевые слова: *разведка, информационно-коммуникационные технологии, интернет.*

А Н А Л И З

НАШ КИБЕРОПТИМИЗМ

Новый номер *Индекса Безопасности* тематический; он посвящен вопросам международной информационной безопасности и глобального управления интернетом. Номер не просто тематический, у него есть несколько особенностей, характерных черт.

Во-первых, тематика номера уникальна для нашего журнала.

Еще ни разу так всесторонне и детально не рассматривались проблемы, связанные с информационными технологиями и их воздействием на социальные процессы как в национальной политике, так и в системе международного мира и безопасности в целом. Эти проблемы сейчас в центре внимания международных организаций, государственных органов, *профильного* бизнеса, экспертных сообществ, исследовательских центров, структур гражданского общества. Диапазон мнений и оценок исключительно широк: от своего рода *кибероптимизма*, превозносящего информационные и коммуникационные технологии едва ли не как главную панацею для решения проблем, накопившихся в экономике и социальной сфере, до намного более пессимистического взгляда, предсказывающего неминуемую *гибель* интернета в привычном виде, его фрагментацию на национальные сегменты и превращение в *почти традиционное* и подконтрольное государственным ведомствам средство массовой информации. Или, точнее, орудие массовой пропаганды и контрпропаганды, идеологического противодействия и противостояния между противоборствующими политическими силами, включая межгосударственные коалиции.

Вообще говоря, в самом широком смысле проблематику данного номера как раз и можно было бы свести к вопросу о соотношении между *оффлайновым* миром и *онлайновым* киберпространством, степени их взаимного проникновения и взаимного влияния. Ведь если исходить из тезиса о том, что проблемы, в том числе правовые и организационные, современных сетевых технологий являются полностью производными от существующих в мире социальных и политических противоречий, то действительно можно предполагать, что таковые технологии на каком-то этапе так или иначе будут полностью поставлены под чей-то контроль. Вопрос будет стоять только в том, чьим будет такой контроль и кто будет способен оспаривать правомерность его принадлежности. И наоборот, если признавать хотя бы относительную самостоятельность информационных технологий в формировании социального портрета современного общества, включая его международно-политический аспект, — а кое-кто активно пытается при этом рассматривать данную тему в контексте *Арабской весны* 2011 г., — то сле-

дует признать, что, как когда-то говорили классики марксизма, *производительные силы начинают обгонять производственные отношения и способны влиять на их трансформацию*. Статьи настоящего номера и посвящены самым разным проявлениям взаимодействия *оффлайна* и *онлайна* в политическом смысле.

Во-вторых, освещаемые в статьях настоящего номера проблемы относительно новы, степень их осознания и изученности пока очень далека от желаемой.

Даже по поводу самих терминов продолжаются достаточно ожесточенные дискуссии как на политическом, так и на научном уровне — является ли объектом международных переговоров и регулирования *информационная безопасность* или *кибербезопасность*, что такое *управление интернетом*, приемлемо ли понятие *multistakeholderism* и как его адекватно перевести на русский язык. Именно поэтому так важно понимать источники возникновения и технические аспекты обсуждаемых проблем, иметь доступ к достоверной информации о способах их решения в разных странах мира. Кому-то может показаться несколько парадоксальной детализация в описании тех или иных особенностей влияния информационных и сетевых технологий на политическую жизнь в статьях номера. Именно поэтому так важно дать правильную оценку *фактологии* политического использования информационных технологий — будь то *цифровая дипломатия* США, опыт регулирования интернета в Китае или воздействие *арабских революций* на формирование информационной политики РФ. И именно такое *многоуровневое* изложение материала является *второй особенностью* предлагаемого читателю номера.

В-третьих, применительно к информационным и сетевым технологиям на самом деле можно говорить, что *история творится на наших глазах*.

В декабре 2012 г. Дубаи примет Всемирную конференцию по международной электросвязи МСЭ. Решения, которые будут на ней обсуждаться и которые неизбежно станут предметом ожесточенных политических дискуссий, перекликаются с проблематикой буквально всех статей номера, и не исключено, к сожалению, что некоторые из сделанных в этих статьях оценок и выводов устареют еще до того, как номер успеет попасть к читателям. Что ж, в этом-то и состоит основная особенность интернета как самой современной технологии коммуникаций — по скорости обмена информацией и возможностям ее оперативного анализа с глобальной Сетью неспособны конкурировать никакие печатные средства массовой информации. Так что, возможно, чтение материалов этого номера можно и нужно совмещать с получением из интернета *последних новостей* в сфере международной информационной безопасности, тем более что до конца календарного 2012 г. в этой сфере ожидается еще много важных событий.

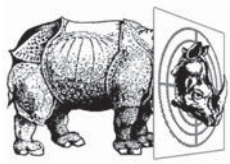
Наконец, *в-четвертых*, лет двадцать назад материалы настоящего номера *Индекса Безопасности* вполне могли быть опубликованы в рубрике *Трибуна молодого ученого*.

Большинство авторов предлагаемых статей — сравнительно молодые эксперты, начинающие свою научную карьеру, но уже продемонстрировавшие достаточную степень зрелости своих представлений о проблематике интернет-технологий и их воздействия на политические реалии. Интернет *молодеет*, и это объективный процесс. Закономерно, что все громче и увереннее звучит голос молодых исследователей, заявляющих о себе как об авторитетных аналитиках и прогнозистах во всем, что касается не только технических, но и социально-политических вопросов развития Сети.

Но разнообразие и острота уже возникших и постоянно возникающих в ходе проникновения интернета в нашу повседневную жизнь новых проблем исключает возможность ситуации, когда кому-то *не хватит работы*. Да, рассматриваемые в этом выпуске журнала проблемы новые, но для эффективного поиска их решений остро востребован и опыт предыдущих поколений, и глубокие специальные знания, и умение реагировать на быстро меняющуюся ситуацию. Тем более когда речь идет о стабильности мировой политической системы и о технологиях, пользователями которых уже сейчас являются миллиарды жителей нашей планеты.

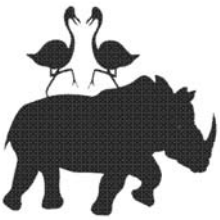
Надеемся, что предлагаемый вниманию наших уважаемых читателей нынешний номер *Индекса Безопасности* сможет быть полезным в решении именно такого рода проблем.

Михаил Якушев
Член Редакционной коллегии



Когда проект будет завершен, бизнесмен в Нью-Йорке сможет диктовать указания, и они будут немедленно появляться в его офисе в Лондоне или любом другом месте. Он сможет со своего рабочего места позвонить любому абоненту на планете, не меняя существующего оборудования. Дешевое устройство, по размерам не больше, чем часы, позволит его обладателю слушать на воде и суше музыку, песни, речи политиков, ученых, проповеди священников, доставляемые на большие расстояния. Таким же образом любое изображение, символ, рисунок, текст могут быть переданы из одного места в другое. Миллионы таких устройств могут контролироваться единственной станцией. И самое главное, что все это будет передаваться без проводов...

Никола Тесла, 1908 г.



Джейми Сондерс:

КАК ИЗБЕЖАТЬ ЭСКАЛАЦИИ КОНФЛИКТОВ В КИБЕРПРОСТРАНСТВЕ?

Необходимы ли изменения российской концепции Конвенции ООН об обеспечении международной информационной безопасности? Возможно ли сегодня создание всеобъемлющего международно-правового режима безопасности киберпространства? Может ли Будапештская конвенция о киберпреступности рассматриваться в качестве потенциальной основы для глобального режима сотрудничества в борьбе с киберпреступностью? Какие терминологические и концептуальные обновления необходимо внести в текст Конвенции Совета Европы, чтобы адаптировать ее к текущей ситуации в области трансграничной киберпреступности? Каковы основные пункты в повестке дня британского МИД в части укрепления международного сотрудничества по вопросам безопасности киберпространства?

Джейми Сондерс, директор по вопросам международной политики в киберпространстве Министерства иностранных дел и по делам Содружества Великобритании, ответил на вопросы корреспондента журнала Индекс Безопасности.

ИНДЕКС БЕЗОПАСНОСТИ: Как Вы оцениваете российскую концепцию Конвенции ООН об обеспечении международной информационной безопасности, которая была представлена на Лондонской конференции по киберпространству в ноябре 2011 г.? Какие изменения необходимо внести в российский проект документа, чтобы он стал прочной основой для дальнейших дискуссий и переговоров о будущем режиме международной безопасности в киберпространстве?

СОНДЕРС: Во-первых, я бы хотел сказать, что мы приветствуем сам факт заинтересованности России в диалоге по данным вопросам. Россия активно участвует в работе Группы правительственных экспертов ООН по анализу ситуации в сфере информации и телекоммуникаций в контексте международной безопасности. Как Вы отметили, российское предложение было представлено год назад на Лондонской конференции по киберпространству, и я ожидаю в этом году двусторонних российско-британских обсуждений, которые были намечены министрами иностранных дел двух стран в мае 2012 г.

Мне кажется, основную озабоченность у нас вызывает вопрос о том, не является ли на данный момент преждевременным само предложение о принятии международного юридически обязывающего документа — это первое. Вторая область, которая вызывает у нас озабоченность — как подходить к решению данных проблем и как избежать эскалации конфликтов в киберпространстве. Нам необходимо найти способ привлечь к данной работе не только правительства, но и саму IT-индустрию, а также гражданское общество, поскольку у всех этих игроков существует серьезная заинтересованность в решении обозначенных вопросов. Они также могут вне-

сти очень важный вклад в плане укрепления доверия, обмена информацией, в том числе в кризисных ситуациях, и в других вопросах.

ИНДЕКС БЕЗОПАСНОСТИ: Не считаете ли Вы, что пришло время для установления юридически обязывающего режима в области информационной безопасности? Ведь мир уже столкнулся с целым рядом деструктивных вирусных атак (*Stuxnet, Flame*, *Duqu*), которые нанесли физический ущерб ключевым объектам инфраструктуры в таких странах, как Иран.

СОНДЕРС: Мы, безусловно, полагаем, что нормы международного права применимы к киберпространству. Я думаю, дальнейшие дискуссии должны сконцентрироваться на вопросе о том, нужны ли нам какие-то новые инструменты, или, может быть, задача состоит в более эффективном применении уже существующих международно-правовых документов (к примеру, законов о ведении вооруженных конфликтов) для решения проблемы кибератак. Я уверен, что существующие механизмы международного права релевантны таким задачам. Поэтому вопрос заключается в том, следует ли нам вести переговоры о создании новых инструментов или сконцентрироваться на более эффективном использовании уже существующих. Мы отдаем предпочтение именно второму варианту.

ИНДЕКС БЕЗОПАСНОСТИ: Может ли Будапештская конвенция о киберпреступности рассматриваться в качестве потенциальной основы для глобального режима сотрудничества в борьбе с киберпреступностью? Какие терминологические и концептуальные обновления необходимо внести в текст Конвенции, чтобы адаптировать ее к текущей ситуации в области трансграничной киберпреступности?

СОНДЕРС: Во-первых, очень важно, чтобы в государствах по всему миру существовало современное законодательство в области противодействия киберпреступности. Во-вторых, необходимы механизмы, обеспечивающие международное сотрудничество в борьбе с компьютерными преступлениями. Мне кажется, большинство государств согласятся с такой постановкой вопроса. На наш взгляд, в Будапештской конвенции даны четкие ответы на вопрос о том, как государствам необходимо действовать. Мы продолжаем поддерживать этот документ и рассматриваем его как хороший образец того, на каких принципах должно основываться качественное национальное законодательство в сфере борьбы с киберпреступностью.

Конечно, Конвенция была принята более 10 лет назад и, согласно распространенному сегодня мнению, нуждается в определенном обновлении. На самом деле механизм для такого обновления заложен в самом тексте Конвенции — а именно в Статье 44. На сей момент никаких обновлений текст конвенции не претерпел. С моей точки зрения, если мы считаем необходимым вносить изменения и поправки в текст Конвенции, нам следует сделать их настолько технологически нейтральными, насколько это вообще возможно. Аналогичный процесс происходит на уровне национального законодательства по борьбе с киберпреступностью — но чем более всеобщим является правовой документ, тем более он долговечен. Хотя, на мой взгляд, очень важен сам факт наличия механизма обновления Будапештской конвенции, притом что такой механизм прописан в Статье 44 самой конвенции, любопытно, что Великобритания до последнего времени не обнаруживала потребности в использовании этого механизма.

ИНДЕКС БЕЗОПАСНОСТИ: Существуют ли какие-то другие потенциальные документы или инициативы, которые, могли бы заменить Будапештскую конвенцию в качестве основы глобального режима по борьбе с киберпреступностью? Способна ли российская глобальная инициатива по борьбе с киберпреступностью, которая может быть обнародована в ближайшее время, заменить собой Будапештскую конвенцию?

СОНДЕРС: Я думаю, важно само содержание Будапештской конвенции, то есть те ее положения, которые обеспечивают основу заложенного в ней механизма трансграничного сотрудничества. Любые будущие предложения в данной сфере будут рассматриваться в сопоставлении с этим базовым уровнем, поэтому если какая-

либо новая инициатива не будет содержать определенных положений, которые на данный момент отсутствуют в Конвенции, но важны с нашей точки зрения, нам будет очень трудно поддерживать такую инициативу. Другими словами, мы рассматриваем Будапештскую конвенцию в качестве действующего стандарта международного сотрудничества по борьбе с киберпреступностью.

Естественно, если будет предложено всеобъемлющее соглашение или другой инструмент, который предложит востребованные на сегодня нормы и более эффективные меры сотрудничества по сравнению с Будапештской конвенцией, мы поддержим такой инструмент. Именно в этом состоит ключевой вопрос: если новые предложения способны предоставить более эффективные механизмы по сравнению с уже имеющейся конвенцией, мы всерьез будем их рассматривать. Если же они попросту не дотягивают до уровня существующих положений Конвенции, у нас возникнут серьезные вопросы в их отношении.

Хочу подчеркнуть, что мы не считаем Будапештскую конвенцию совершенным документом. В этой области есть еще над чем работать, и именно с этой точки зрения мы будем рассматривать все новые инициативы. Хотелось бы также добавить, что между Россией и Западом существует не так уж много противоречий касательно того, как добиться желаемого результата в области борьбы с киберпреступностью на международном уровне. Однако я полагаю, что соглашение с Россией должно содержать акцент на совершенствование системы международного сотрудничества по борьбе с киберпреступностью и обеспечивать соответствующую среду для поддержания стабильности всего киберпространства. Не думаю, что у нас есть какие-то фундаментальные разногласия по поводу того, какими мы видим желаемые плоды нашего сотрудничества.

ИНДЕКС БЕЗОПАСНОСТИ: Камнем преткновения между Россией и ее западными партнерами при обсуждении проблем киберпространства являются существенные терминологические и концептуальные расхождения. Российские эксперты предпочитают вести речь об *информационной безопасности*, а не о *кибербезопасности.* Какой из этих двух подходов Вам представляется более рациональным для целей международного регулирования киберпространства? Есть ли шансы на то, что российская концепция информационной безопасности будет понята и принята на Западе, в частности в Великобритании?

СОНДЕРС: Здесь нужно различать два отдельных аспекта. Первый аспект — это вопрос языка и терминологии. Я согласен с тем, что этот аспект уже привнес определенные трудности, способные затормозить развитие международного диалога. Я думаю, чтобы добиться определенного прогресса, нам — то есть Великобритании, России и другим игрокам — нужно четко объяснить друг другу то значение, которое мы вкладываем в наши определения и термины. Конечно, здесь также существуют определенные трудности перевода, так что нужно постараться прийти к единому набору определений и терминологии.

В данный момент нам часто приходится лишь догадываться о том, что же на самом деле имеет в виду наш партнер. Чем более четко мы сможем объяснить смысл наших идей и предложений, тем меньше мы будем зацикливаться на терминах и тем лучше мы сможем понять глубинный смысл этих предложений. Не думаю, что нам удастся выработать общий набор определений и терминов в краткосрочной перспективе — но мы можем, по крайней мере, понять, какой смысл мы вкладываем в разные термины. Это поможет нам определить, где именно между нами на самом деле существуют разногласия, а где каждый из нас просто не до конца понимает, о чем ведет речь партнер.

Нужно, однако, отметить, что за разной терминологией иногда скрываются и реальные разногласия. Это, в частности, касается предлагаемой тематики международной дискуссии по вопросу безопасности. Если британские политики и эксперты не истолковали превратно смысл российской фразеологии, можно утверждать, что термин *информационная безопасность*, который широко используется рос-

сийской стороной, включает само по себе информационное наполнение коммуникаций. Поэтому основной вопрос в рамках международного диалога на эту тему сводится к тому, что российский подход предполагает такие ограничения свободы слова в киберпространстве, которые, на наш взгляд, противоречат обязательствам, взятым на себя обеими нашими странами в рамках Всеобщей декларации прав человека и Международного пакта о гражданских и политических правах. Эти документы подписали и Великобритания, и Россия. Поэтому важно понять смысл, который мы вкладываем в используемые термины, и постараться определить, действительно ли мы говорим о различающихся подходах, или все дело в том, что мы неправильно поняли друг друга. При этом не следует преуменьшать различия в наших взглядах, которые на самом деле существуют — особенно это касается вопроса информационного наполнения коммуникаций.

ИНДЕКС БЕЗОПАСНОСТИ: Считает ли британское правительство новые крайне сложные виды вредоносных программ типа *Stuxnet* и *Flame* угрозой национальной безопасности? Какие шаги предпринимает британский МИД для продвижения дискуссии по данной проблеме на международном уровне?

СОНДЕРС: Во-первых, Вы отдельно выделили в своем вопросе вирусы *Stuxnet* и *Flame.* Я бы не сказал, что мы считаем именно эти киберинструменты отдельной угрозой для нашей национальной безопасности. Но мы осознаем, что вредоносные программы в целом представляют собой угрозу, или потенциальную угрозу, и в этом смысле их можно воспринимать как угрозу национальной безопасности. Современные вредоносные программы действительно способны нанести весьма существенный ущерб критическим объектам национальной инфраструктуры. Великобритания пока не сталкивалась с вирусами типа *Stuxnet* или *Flame*, нацеленными конкретно против ее систем и объектов. Но это не отменяет того факта, что вредоносные программы могут нанести серьезный ущерб нашей критической инфраструктуре. Мы хорошо осознаем этот факт.

Что касается необходимых мер реагирования на такие угрозы, то мы, естественно, очень активно участвуем в работе Группы правительственных экспертов ООН по вопросам безопасности в киберпространстве. Мы также поддерживаем деятельность в этом направлении в рамках ОБСЕ и Регионального форума АСЕАН (АРФ). Что касается мер по укреплению доверия, мы считаем, что это очень важная и нужная тема для межправительственных дискуссий. С моей точки зрения, перед нами стоит общая цель: предотвратить наращивание разрушительного потенциала вредоносных программ и не допустить нанесения ущерба критической национальной инфраструктуре.

Наконец, стоит также упомянуть, что мы принимали проведенную в 2011 г. Лондонскую конференцию по киберпространству. Один из основных вопросов, обсуждавшихся на конференции, касался именно угрозы, которую представляют собой разрушительные вредоносные программы для наших критических объектов и систем. Данный вопрос вновь был вынесен в повестку Будапештской конференции по киберпространству (4–5 октября 2012 г.), равно как и всех основных мероприятий в области кибербезопасности, запланированных на будущий 2013 г. Я не утверждаю, что это единственная проблема, заслуживающая серьезного рассмотрения, но ее важно обсуждать именно на уровне правительств, чтобы привлечь к этим вопросам внимание политического руководства наших стран.

ИНДЕКС БЕЗОПАСНОСТИ: Вы отметили, что вредоносные программы считаются серьезной угрозой для критической национальной инфраструктуры. Какие сегменты этой инфраструктуры наиболее уязвимы? Энергосети, банковские информационные системы или какие-либо иные объекты?

СОНДЕРС: Это очень сложный вопрос, в котором сочетаются два аспекта: степень уязвимости самих систем и роль этих систем в обеспечении общественных процессов. Поэтому невозможно составить какой-то список наиболее уязвимых или наиболее важных сегментов критической национальной инфраструктуры.

Но очевидно, что есть определенные сегменты, в том числе электрические сети и энергосистемы, системы обеспечения страны продовольствием, которые требуют наиболее прочных гарантий того, что система обладает должным уровнем безопасности и надежно защищена. Мы анализируем состояние нашей критической инфраструктуры по отдельным секторам, чтобы определить, где существует наибольшая вероятность возникновения проблем и где перед нами стоят самые сложные задачи. Я также считаю, что важно не пытаться рассматривать киберугрозы в отрыве от всех остальных угроз. Нам нужно защищать такие системы, как электросети, от широкого спектра угроз — как стихийного, так и техногенного характера, как компьютерных, так и всех остальных. Поэтому мы стремимся к целостному и всестороннему анализу ситуации.

ИНДЕКС БЕЗОПАСНОСТИ: Когда речь идет о массированных и хорошо спланированных кибератаках, ключевой проблемой является анонимность их авторов. Подвергались ли британские правительственные компьютерные сети таким атакам и удавалось ли определить их источник? Обвиняло ли когда-либо британское правительство какие-либо конкретные государства в том, что они несут прямую ответственность за кибератаки?

СОНДЕРС: Во-первых, Великобритания, как и многие другие страны, регулярно подвергается попыткам вторжения в ее компьютерные сети. Я полагаю, что ранее уже звучали конкретные цифры, характеризующие атаки на сети государственного сектора — сети некоторых ведомств подвергались тысячам атак. Так что, как видите, объем вредоносной сетевой деятельности весьма велик, и определить, кто стоит за такими атаками, трудно, однако эта задача не является принципиально невыполнимой. Пока что мы решили не обвинять какие-либо конкретные страны в том, что они несут ответственность за кибератаки. На официальном уровне мы таких публичных заявлений не делаем. Однако нужно понимать, что если мы имеем основания подозревать какую-либо страну в подобной деятельности, то у нас есть право предпринять ответные меры, в соответствии с нашими правами и обязанностями, закрепленными в международном праве. Если мы полагаем, что наши системы подверглись нападению, то мы, естественно, предпринимаем соответствующие шаги.

ИНДЕКС БЕЗОПАСНОСТИ: Входят ли в число таких ответных шагов дипломатические или военные меры?

СОНДЕРС: Реагирование будет происходить на самых разных уровнях и, естественно, будет включать определенные шаги на дипломатической арене. Наша реакция на кибернападение не будет ограничиваться лишь принятием каких-либо технических мер, направленных на устранение уязвимости компьютерных систем. Речь будет идти и о других ответных мерах, в том числе дипломатического характера, если это будет целесообразно.

ИНДЕКС БЕЗОПАСНОСТИ: Каковы основные пункты в повестке дня британского МИД в части укрепления международного сотрудничества по вопросам международной информационной безопасности? Планирует ли сама Великобритания в ближайшее время представлять какие-то новые глобальные инициативы или перспективные стратегии в данной сфере?

СОНДЕРС: Я бы хотел особо отметить два момента в данном случае. Первый из них состоит в том, что, с моей точки зрения, необходимо проделать большую работу над повышением уровня информированности общественности и конкретных социальных групп по поводу проблем, связанных с киберпространством. Такая работа, в частности, должна вестись на высшем уровне государственного руководства и бизнеса, а также среди гражданского общества в различных странах. Естественным сегментом целевой аудитории являются бизнес-лидеры по всему миру. Все мы хорошо понимаем, что столкнулись с серьезной угрозой в данной области. Как я уже упоминал, наша прошлогодняя конференция в Лондоне стала практической площадкой для отработки подобного подхода. Мы регулярно обсуж-

даем эту проблему с партнерами, чтобы повысить их информированность о ситуации, предложить им свою помощь и т. д. На самом деле такой стране, как Великобритания, есть что сказать своим партнерам во всем мире, чтобы подтолкнуть их к осознанию того, что киберугрозы представляют собой серьезный вызов и этот вызов необходимо сдерживать сообща.

Второе направление, которому мы уделяем внимание, включает передачу уже накопленных нами опыта и знаний другим странам, с тем чтобы помочь им в развитии собственного потенциала в данной области. Мы уже финансируем целый ряд инициатив, в рамках которых передаем другим странам не только финансовые средства, но и собственный опыт. Однако мы считаем, что должны делать в данном направлении еще больше, поэтому в сентябре-октябре 2012 г. нам предстоит провести анализ того, какой дополнительный вклад мы можем внести в программы по развитию собственного национального потенциала других стран, как сделать эти масштабные программы укрепления потенциала борьбы с киберугрозами более эффективными. Для нас также важно удостовериться в том, что мы оказываем необходимое влияние на глобальную повестку в области укрепления потенциала противодействия киберугрозам.

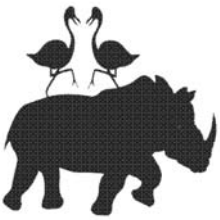
ИНДЕКС БЕЗОПАСНОСТИ: Существуют ли у Великобритании какие-либо конкретные региональные приоритеты в международном сотрудничестве по укреплению кибербезопасности?

СОНДЕРС: Выделить подобные приоритеты непросто, поскольку различные сценарии в регионах требуют разных шагов и подходов. Естественно, высшим приоритетом для нас является обеспечение безопасности *наших собственных* информационных систем. Однако мы также уделяем значительное внимание тем странам, которые больше всего нуждаются в нашей помощи. Некоторые из них — и здесь я, в частности, привожу тот случай, когда мы выделяем финансирование на программы в данной области — расположены в Юго-Восточной Европе, и мы сотрудничаем с ними через механизмы Евросоюза. Мы также финансируем работу Совета Европы по оказанию содействия тем странам, которые стремятся укреплять свое национальное законодательство в области кибербезопасности. Мы поддерживаем работу в рамках Содружества наций, направленную на укрепление потенциала и расширения возможностей правоприменительной практики применительно к сфере кибербезопасности. Но это лишь начало, и нам предстоит сделать намного больше, в том числе предпринимать более энергичные усилия именно в тех областях, где они способны принести максимальную отдачу, на которую мы рассчитываем. Нас, в частности, беспокоит, что ведется довольно много различных программ, которые не приносят ожидаемых результатов.

Я бы также хотел вернуться к Вашему предыдущему вопросу относительно международных обсуждений на тему законов и глобальных соглашений в области кибербезопасности. Такие обсуждения уже ведутся, однако есть еще одна область, играющая важную роль в развитии международного сотрудничества в данной сфере. Речь идет об укреплении доверия, повышении прозрачности и подобных мерах, которые создают благоприятный климат для международного сотрудничества в борьбе с общими киберугрозами.

ИНДЕКС БЕЗОПАСНОСТИ: Каковы ключевые приоритеты британского МИД в сфере сотрудничества с Россией по вопросам кибербезопасности?

СОНДЕРС: Во-первых, мы весьма искренне приветствуем участие в этих дискуссиях российских неправительственных организаций, а также российского бизнеса. Мы считаем, что их роль и вклад очень важны. Мне кажется, чем больше мы говорим друг с другом и чем шире круг совместно обсуждаемых проблем и сюжетов, тем больше вероятность того, что нам удастся найти точки соприкосновения и добиться прогресса. И я надеюсь, что ПИР-Центр воспримет этот посыл как всестороннюю поддержку своей работы в рамках проекта по информационной безопасности и управлению интернетом.



Андрей Колесников:

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РФ: СЛОЖНОСТИ И ПЕРСПЕКТИВЫ

Проблемы отражения киберугроз, защиты критической инфраструктуры, развития доменного пространства и обеспечения безопасности в интернете выходят на первый план в российской повестке дня. Эксперты, бизнес-лидеры и дипломаты стремятся понять, что ждет кириллическую доменную зону, требуется ли России новый доктринальный базис для обеспечения эффективной политики кибербезопасности и достигают ли своей цели недавние новации в отечественном законодательстве о безопасном интернете. Каковы приоритеты в перечисленных областях у администратора национальных доменов верхнего уровня .ru и .рф — Координационного центра национального домена сети Интернет (КЦ НДСИ)? Об этом мы побеседовали с директором КЦ НДСИ Андреем Колесниковым.

ИНДЕКС БЕЗОПАСНОСТИ: Координационный центр принимает активное участие в продвижении ряда сюжетов в области развития информационных технологий в РФ. Попадают ли в повестку КЦ НДСИ вопросы информационной безопасности, и если да, то в каком ключе? В частности, видит ли Координационный центр перед собой задачу участия в совершенствовании национального законодательства в области информационной безопасности, безопасного интернета?

КОЛЕСНИКОВ: Действительно, Координационный центр исторически принимает активное участие в обсуждении и решении вопросов обеспечения безопасности как в области интернет-инфраструктуры, так и в сфере информационной безопасности, хотя некоторые из этих функций и не вытекают напрямую из названия и уставных документов нашей организации. Однако все эти вопросы являются неотъемлемой частью обеспечения функционирования интернета, а наша непосредственная обязанность прежде всего состоит в обеспечении непрерывности оказания услуг доменной адресации, а также функционирования сети DNS российского сегмента интернета. Установленный показатель — 100% работоспособности разрешения доменных имен в зонах *.ru* и *.рф* вне зависимости от внешних и внутренних ситуаций. Второй важной областью деятельности КЦ НДСИ является анализ использования доменных имен в незаконных целях и борьба со *зловредами* (буквальный перевод англ. *malware*, вредоносные зловредные программы. — *Ред.*). К числу основных видов деятельности, предполагающей использование программного кода в злонамеренных целях, сегодня относится создание ботнетов, вирусов, а также фишинг и кибермошенничество. Координационный центр постоянно участвует в различных инициативах, в том числе законодательных, для повышения общего уровня кибербезопасности в Российской Федерации и противодействия данной деятельности.

ИНДЕКС БЕЗОПАСНОСТИ: Какие проекты и инициативы, связанные с повесткой информационной безопасности, развивает или планирует развивать в ближайшем будущем Координационный центр? Ведется ли сотрудничество Координационного центра с госорганами и экспертным сообществом, и если да, то по каким направлениям и каковы его результаты на сегодняшний день?

КОЛЕСНИКОВ: Одной из самых первых инициатив Координационного центра в области информационной безопасности был *День безопасного Интернета*, который впоследствии превратился в *Год безопасного Интернета*. Эта инициатива, которую мы начали совместно с Фондом Развития Интернет (ФРИ) в 2008 г., была поддержана многими компаниями-операторами и *хостерами*. По сути, именно она стала основой для множества других общественных инициатив, включая создание такой организации, как *Лига безопасного интернета*. КЦ НДСИ впервые предложил серьезные поправки в понятийный аппарат российских нормативно-правовых актов, так или иначе затрагивающих проблематику интернета, три года назад, в 2009 г. Однако на тот момент в силу различных обстоятельств предложенные поправки так и не были приняты.

Сегодня эксперты КЦ входят в различные рабочие группы, задействованные в работе по повышению качества законодательной базы в сфере информационной безопасности. Последний пример — принятие 139-ФЗ от 28 июля 2012 г.[1] и наши конкретные предложения касаются переноса фокуса фильтрации контента в соответствии с положениями закона с *уровня кабелей* на уровень интернет-приложений. В текущие поправки, которые были разработаны Российской ассоциаций электронных коммуникаций (РАЭК) и которые были поддержаны Координационным центром, наши предложения не вошли, так как они требуют расширения фактуры закона. Но рано или поздно методы и технологии приведут нас к подобным решениям — ведь речь идет о неизбежной эволюции интернета.

В части взаимодействия с правоохранительными органами нашим главным государственным партнером является Министерство связи и массовых коммуникаций РФ. КЦ НДСИ играет роль *центра компетенций* по многим вопросам, связанным с обеспечением безопасного функционирования сети интернет. Другим направлением в рамках деятельности Координационного центра является сотрудничество с МВД РФ и другими правоохранительными органами в рамках борьбы с киберпреступностью.

ИНДЕКС БЕЗОПАСНОСТИ: Видите ли Вы потребность в обновлении или пересмотре российской нормативной и доктринальной базы в области информационной безопасности на сегодняшний день? Если да, какие подходы и решения должны составлять основу такого документа? Предпринимает ли КЦ НДСИ какие-то действия в этом направлении?

КОЛЕСНИКОВ: С точки зрения экспертов Координационного центра, в России на сегодняшний день отсутствует сформулированный и закрепленный в каком-либо доктринальном или нормативно-правовом акте целостный подход к национальной проблематике кибербезопасности. Существует лишь ряд разрозненных документов, в которых просматриваются интересы различных ведомств в получении контроля над той или иной областью деятельности, такой как защита критической инфраструктуры, лицензирование операторов и т.д. Что касается Доктрины информационной безопасности Российской Федерации от 2000 г., добавить к ней что-либо и провести ее *модернизацию* не представляется возможным, так как документ морально устарел. В России не существует формального списка угроз безопасности киберпространства и матрицы приоритетов, необходимой для адекватной оценки этих угроз и управления ими.

Мы изучили опыт 11 ведущих *кибердержав* и пришли к неутешительному выводу: Российская Федерация серьезно отстала в области разработки и внедрения единых методов и стандартов обеспечения кибербезопасности. В Стратегии национальной безопасности Российской Федерации до 2020 г. и упомянутой Доктрине

повестке кибербезопасности практически не нашлось места. В частности, не урегулированы и нормативно не закреплены проблемы оперативной реакции на инциденты в информационных сетях, использование интернета в криминальных целях и т.д. Подход к этой проблематике должен принципиально отличаться от традиционных для России практик с выраженным приоритетом роли специальных служб и вооруженных сил. Например, в вышеупомянутой Стратегии определено, что национальную безопасность обеспечивают именно армия и силовые структуры; практически идентичный посыл несет Доктрина.

Нам нужен другой подход, близкий к тем, которые сегодня используются в Великобритании и других странах Евросоюза, в США, Китае, Японии, Бразилии и многих других странах. Кибербезопасность должны обеспечивать все участники национальных интернет-отношений сообща — от рядовых пользователей до руководителей страны. Что особенно важно, в обеспечении кибербезопасности должен принимать активное участие бизнес.

В этой связи России необходима прежде всего *Стратегия кибербезопасности* верхнего, национального уровня, в которую будет входить список из конечного и конкретного списка задач, которые необходимо решать, а также сроки, к которым их надо решить. Нужны не общие слова, а конкретика. И исполнителями этой стратегии должны быть не только государственные органы и органы власти, а все задействованные и заинтересованные стороны, включая граждан в частном качестве. Зачатки этого подхода можно увидеть в недавнем документе по вопросам защиты объектов критической инфраструктуры[2]. Хотя и в нем, опять-таки, *торчат уши* вполне конкретных ведомств, а указанные ориентиры по срокам вызывают удивление. Так, появление в России системы обнаружения кибератак на критическую информационную инфраструктуру запланировано только в период с 2017 до 2020 г., то есть через пять-восемь лет! Между тем уже два года назад вирус *Stuxnet* показал, какой ущерб может быть нанесен критической инфраструктуре лишь при помощи компьютерного кода. Следует помнить о том, что за прошедшее время арсенал кибероружия лишь увеличился и обогатился еще более сложными разработками. В то же время российская критическая инфраструктура сложнее и *разветвленнее* иранской, и уже поэтому нам следует быть готовыми к отражению подобных угроз сейчас, а не в среднесрочной перспективе.

ИНДЕКС БЕЗОПАСНОСТИ: 12 июля 2012 г. на сайте Совета безопасности РФ был опубликован очередной документ[1], посвященный вопросам защиты критической инфраструктуры в РФ. Входят ли вопросы безопасности критической инфраструктуры, включая инфраструктуру глобальной сети и ее российского сегмента, в круг приоритетов КЦ НДСИ? Какие угрозы безопасности инфраструктуры интернета существуют в РФ в настоящее время?

КОЛЕСНИКОВ: Координационный центр обеспечивает работоспособность одного из главных критических элементов инфраструктуры Сети — системы доменной адресации. При этом специалисты КЦ стабильно демонстрируют стопроцентную доступность сервиса, что является одним из наших ключевых приоритетов. Используя передовые технологические и методические подходы к построению географически распределенного сервиса, мы полностью исключили возможность злонамеренного влияния на сети извне и изнутри. В ближайшее время мы поднимем уровень доверия и защиты от подмены доменных ресурсов внедрением протокола DNSSEC [Domain Name System Security Extensions], обеспечивающего цепочки доверия между серверами DNS. Хотелось бы выразить надежду, что основные стратегические инфокоммуникационные системы в Российской Федерации используют столь же надежные методы и подходы.

Мы считаем, что проблематика кибербезопасности выходит далеко за пределы вопросов регламентирования доступности государственных служб и структур через интернет, равно как и сетевого обмена для обеспечения информационного взаимодействия госструктур. Напротив, доступность и безопасность электронных коммуникаций потребителей с банками и другими финансовыми учреждениями,

системами интернет-торговли, системами электронных платежей, ведущими СМИ, социальными сетями, мультимедийными порталами и другими интернет-сервисами вызывает бо́льшую озабоченность у общества, чем недоступность, например, сайта органа федеральной или муниципальной власти.

Оценивая актуальность тех или иных проблем в российской повестке кибербезопасности, мы бы предложили следующую иерархическую шкалу:

- во-первых, отсутствие стратегических планов решения проблем кибербезопасности, отсутствие единой политики кибербезопасности России и опасность внутриведомственной борьбы в этой области;
- во-вторых, отсутствие единого механизма управления вопросами кибербезопасности в России
- в-третьих, низкая грамотность в области безопасного использования интернета, как дома, так и на работе;
- в-четвертых, отсутствие законодательно закрепленных требований по обеспечению безопасности информационной инфраструктуры бизнеса, в том числе в критически важных областях, например в сфере инфокоммуникаций;
- наконец, как следствие вышеперечисленного, отсутствие последовательной и *прагматичной* внешней политики в области управления интернетом, направленной на защиту конкретных интересов Российской Федерации в трансграничном киберпространстве.

ИНДЕКС БЕЗОПАСНОСТИ: Насколько успешным и оправданным Вы считаете опыт внедрения и использования кириллической доменной зоны *.рф*? Каковы перспективы дальнейшего развития кириллического сегмента Рунета? Считаете ли Вы повсеместное развитие локальных алфавитных доменных зон, таких как кириллическая, арабская и иероглифическая — фундаментальной тенденцией развития интернета, и если да, не повлечет ли она фрагментацию и потерю единства глобальной сети?

КОЛЕСНИКОВ: Запуск домена *.рф* для Российской Федерации, а также иероглифической доменной зоны. 中国 для КНР, арабской доменной зоны и других корневых доменов на национальных языках, а точнее алфавитах, отражает естественный процесс эволюции адресного пространства интернета. При этом данный процесс не несет в себе фундаментальной тенденции потери единства глобальной сети. Мы сталкиваемся с действием своеобразного *фактора Вавилона,* перенесенного в виртуальное пространство. Здесь важно помнить, что Рунет говорит по-русски со времен своего появления, и появление кириллических доменов лишь закрепляет языковую специфику российского сегмента Сети, не придавая ему каких-либо фундаментально новых качеств.

Домен *.рф* с момента запуска является одним из наиболее успешных среди, с одной стороны, проектов интернационализированных нелатинских доменов верхнего уровня, а с другой стороны — проектов развития Рунета, к воплощению которых был непосредственно причастен КЦ НДСИ. Главная проблема интернет-компаний, госструктур и пользователей в странах, работающих с интернационализированными нелатинскими доменами верхнего уровня, заключается в опыте использования программ и приложений, задействованных в интернете, таких как электронная почта, поисковые машины, приложения социальных сетей и т.д. Такая проблема характерна не только для Рунета, но и для интернет-сегментов КНР и арабских стран. Однако я считаю, что это всего лишь вопрос времени и уже через два-три года никто не заметит разницы в обработке названий доменов на латинице и на нелатинских алфавитах.

ИНДЕКС БЕЗОПАСНОСТИ: Какова позиция Координационного центра в отношении недавно принятого закона 139-ФЗ? Какое техническое решение в отношении

блокировки контента, подпадающего под запрет в соответствии с положениями закона, Вы считаете оптимальным? В частности, как Вы оцениваете организационную, финансовую и техническую готовность российского интернет-сектора к широкому применению технологии DPI (deep packet inspection) с целью соблюдения положений 139-ФЗ?

КОЛЕСНИКОВ: *Во-первых*, мы считаем появление закона в отношении защиты детей воплощением закономерного *социального заказа* граждан России. Формирование такого заказа является знаком того, что интернет стал частью повседневной жизнь большинства граждан России. *Во-вторых,* имплементация этого заказа в букве закона в разделе, регламентирующем доступ к онлайн материалам, представляется Координационному центру неверной в части выбора алгоритма ограничения доступа к материалам, подпадающим под запретительные нормы законодательства. Мы считаем, что появление фильтров-посредников между *источник*ом и *потребителем,* логически, технологически и юридически не связанных ни с первым, ни со вторым, может повлечь труднопредсказуемые последствия с точки зрения организации и функционирования интернет-связи. Кроме того, подобный способ ограничения доступа абсолютно неэффективен в отношении организации связи с использованием защищенных протоколов и *туннелей* HTTPS/SSL и других подобных средств.

Но самой главной логической ошибкой в выборе метода блокировки мы считаем игнорирование того факта, что сегодняшняя Сеть предоставляет практически неограниченные возможности для бесплатного воспроизведения и тиражирования (репликации) контента, доступ к которому предполагается блокировать по тому или иному конкретному адресу в интернете. При этом в законе полностью отсутствуют какие-либо методы борьбы с *первоисточником*, то есть непосредственным производителем подобного рода материалов. Мы полагаем, что 139-ФЗ должен эволюционировать, чтобы превратиться в эффективное орудие защиты детей от ненадлежащего контента в Сети. Чтобы закон мог исполнять такую функцию, в само его *тело*, равно как и в подзаконные акты, в дальнейшем необходимо будет вносить определенные коррективы. Такие коррективы должны быть направлены прежде всего на использование фильтрации на абонентских устройствах и на уровне интернет-приложений, обеспечивающих потребителя информацией: поисковых машин, интернет-браузеров, семейных фильтров, встроенных в операционные системы, и т.д. При этом фильтрация контента должна быть максимально *смысловой* и в минимальной степени зависеть от инфраструктуры и места размещения незаконного контента. Мы активно сотрудничаем с Лигой безопасного интернета в выборе наиболее действенных методов смысловой категоризации информации в интернете и ведем достаточно активную лабораторную деятельность по изучению новых методов определения тематической составляющей с такими учеными, как Симон Кордонский и Валерий Бардин.

Думаю, что техническая готовность к исполнению закона будет обеспечена без особых проблем, так как у операторов есть возможность выбора методов фильтрации. Злоупотребления и неточность исполнения будут видны моментально. Но неблагодарное дело строить предположения, пока не появилась практика исполнения этого закона. В любом случае необходимо будет смотреть на конкретные случаи применения закона в течение достаточно длительного времени, как минимум одного года. Очевидно, что оператором так называемого реестра *черного списка* будет Лига безопасного интернета, так как именно эта организация выступает локомотивом внесения ограничений в интернете для детей. И, по всей видимости, тема *списков* будет развиваться и, как мне кажется, следующий логичный шаг — это переоценка методов, используемых в *школьной* фильтрации.

Подход, который предписывает операторам *закрывать* доступ к ресурсам, предполагает использование оборудования, необходимого для глубокой проверки информационных пакетов (DPI) и обещает быть весьма затратным. Очевидно, что закон и его разработчики нуждаются в постоянной *обратной связи* с представителями интернет-сектора и экспертного сообщества, для корректировки слабых мест

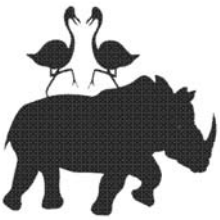
в тексте закона и повышения эффективности методов фильтрации. Необходимо также следить за случаями неизбирательного применения. Крайним примером здесь мог бы служить принцип блокировки противоправного контента по доменному имени. В случае с ФЗ-139 речь шла бы о полной остановке деятельности таких крупных сервисов и ресурсов, как *LiveJournal, YouTube, Facebook, Twitter* на территории Российской Федерации из-за единственной записи в аккаунтах кого-либо их пользователя, которая нарушала бы положения закона и не была бы удалена вовремя. Мы с интересом следим за развитием сюжета, связанного с размещением фильма *Невинность мусульман* на *YouTube*.

К сожалению, в России имеются прецеденты временной блокировки подобных ресурсов из-за несоответствия контента, загруженного пользователями, нормам российского законодательства. И хотя до сих пор такие случаи не были связаны с действием 139-ФЗ, каждый из них наносил определенный ущерб интернет-сектору. Даже сутки блокировки *LiveJournal* в отдельно взятом регионе чреваты для сервиса значительными репутационными и финансовыми рисками. В этом смысле чрезвычайно важно уточнить нормы 139-ФЗ на уровне подзаконных актов, чтобы свести к минимуму *сопутствующий ущерб* от применения закона и *неизбирательную* блокировку крупных сервисов, не несущих ответственности за действия пользователей. В этой связи Координационный центр поддерживает разработанные РАЭК и компанией *Яндекс* поправки к 139-ФЗ, так как их цель состоит в сокращении неизбежного ущерба от подобного применения 139-ФЗ.

Примечания

[1] Федеральный закон Российской Федерации от 28.06.2012. № 139-ФЗ «О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации».

[2] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Информационная безопасность, Национальная безопасность России. Совет Безопасности Российской Федерации, http://www.scrf.gov.ru/documents/6/113.html (последнее посещение — 11 сентября 2012 г.).



Крис Палларис:

НОВЫЕ ТЕХНОЛОГИИ В РАЗВЕДКЕ

Могут ли инструменты предиктивной аналитики предсказывать рабочий график В.В. Путина? В чем заключается основное отличие разведки из открытых источников от традиционной разведывательной деятельности, которой занимаются в основном государственные секретные службы? Какие факторы подстегнули развитие коммерческой разведки из открытых источников? Какое место в такой разведке играют информационно-коммуникационные технологии?

На вопросы корреспондента журнала Индекс Безопасности отвечает Крис Палларис, директор и главный консультантом компании i-intelligence. Компания работает с государственными и частными организациями, помогая им развить свой потенциал в области стратегической коммерческой разведки и сбора информации, а также обучая их персонал эффективной работе в постоянно меняющихся внешних условиях.

ИНДЕКС БЕЗОПАСНОСТИ: Коммерческая разведка из открытых источников является достаточно новым видом деятельности. Какие факторы подстегнули ее развитие — как для Вашей компании, так и для всего европейского рынка? Каким Вам видится будущее разведки из открытых источников в течение следующих трех-пяти лет?

ПАЛЛАРИС: Вопреки широко распространенному мнению, коммерческая разведка не является новой дисциплиной. Истоки ее можно проследить как минимум до XVII в. и Ост-Индской компании. Я подозреваю, что первые примеры такой деятельности появились еще раньше.

В своей нынешней форме коммерческая разведка появилась после окончания холодной войны. Благодаря спаду напряженности в международных отношениях тысячи профессионалов в области разведки пришли в частный сектор, предлагая тем отраслям промышленности (энергетика, финансы, фармацевтика, и т. д.), у которых хватило здравого смысла воспользоваться их услугами, свой уникальный набор знаний, умений и навыков. Со временем эти профессионалы организовали собственные консалтинговые компании.

В настоящее время на рынке присутствуют самые разнообразные фирмы, специализирующиеся на коммерческой разведке — от крупных компаний, которые работают во многих отраслях промышленности, до небольших высокоспециализированных организаций, работающих в узкой отрасли или даже на одного-единственного клиента. Сама отрасль уже превратилась в глобальный феномен. Везде, где зарабатываются деньги, существует необходимость в информации — хотя бы для того, чтобы свести к минимуму риски и по максимуму использовать коммерческие возможности.

Компании, работающие в нашей отрасли, отличаются своей специализацией и конкретной сферой работы. К примеру, *i-intelligence* специализируется на тренинге и консультировании клиентов, которые желают за небольшие деньги приобрести собственный конкурентоспособный потенциал в области сбора информации, используя при этом широко доступные инструменты и технологии. Иными словами, существует столько же разных видов коммерческой разведки, сколько существует областей, где могут применяться наши знания и умения.

Интернет и широкое распространение IT-технологий сыграли значительную роль в стимулировании роста данной отрасли. Количество всевозможных источников информации продолжает расти настолько быстрыми темпами, что большинство организаций за этим ростом просто не поспевают. К примеру, типичному отделу продаж коммерческой компании приходится вести мониторинг сотен отдельных субъектов (клиенты, конкуренты, и т. д.), черпая информацию из десятков источников, в том числе из открытых социальных сетей в интернете и баз данных с ограниченным доступом. Конечно же, интернет не является единственным источником данных для конкурентной коммерческой разведки. Более того, иногда он даже не является наилучшим из имеющихся источников. Но он незаменим в плане изучения рынка и конкурентной среды. К сожалению, большинство организаций не знают, как воспользоваться возможностями интернета с наибольшей отдачей. Не знают этого и те выпускники университетов, на которых такие организации часто возлагают свои надежды в данной области. В результате многие функции по текущему сбору данных и информации часто передаются внешним организациям в рамках аутсорсинга.

Технология тоже сыграла свою роль. Когда я только начинал свою карьеру в Лондоне, единственным типом компьютеров были настольные рабочие станции. При этом возможности этих станций были ограничены тем набором программного обеспечения, который на них решил установить работодатель. Сегодня компьютер, который помещается в ваш карман, является самым лучшим средством коммерческой разведки — лучшего не купишь ни за какие деньги. Этот компьютер может снимать фотографии и видео, он может записывать беседы с экспертами в необходимой отрасли, он помогает в геолокации новых и уже существующих клиентов. Его функциональность определяется только вашим собственными потребностями и вашей способностью найти нужное для работы программного обеспечения (ПО). Однако даже в данной сфере многие организации плохо себе представляют, как можно использовать эти инструменты и технологии себе во благо, не нарушая при этом никаких законов.

Откровенно говоря, очень многие поставщики услуг в сфере коммерческой разведки с удовольствием эксплуатируют такую безграмотность своих клиентов. Несколько месяцев назад у меня был ланч с представителем одной компании-энерготрейдера. Он утверждал, что поставщик услуг в области коммерческой разведки, нанятый этой компанией, имеет доступ к информации, которую невозможно найти в интернете. На самом деле эта информация в интернете есть, главное — знать, где ее искать. Фактически, фирма обманным путем убедила своего клиента платить ей десятки тысяч долларов за информацию, которую можно было раздобыть бесплатно с помощью мышки и клавиатуры.

Разработчики технологий ведут себя похожим образом — хотя и не все, но довольно многие. К примеру, большинство фирм, специализирующихся на мониторинге СМИ, продают своим клиентам доступ к инструментам и технологиям, которые сильно уступают в эффективности бесплатным инструментам, имеющимся в свободном доступе в интернете. На самом деле все что нужно, чтобы организовать первоклассный мониторинг СМИ или приобрести вполне конкурентоспособный потенциал в области коммерческой разведки — это учетная запись в *Google*.

Что касается тенденций, то одной неизбежной закономерностью, определяющей развитие рынка, является постоянное увеличение потока информации. Потребность в информации и спрос на нее будут расти и далее в обозримом будущем. Давайте, к примеру, рассмотрим те проблемы, с которыми в наше время сталкивается любая компания: постоянная экономическая неопределенность, меняющаяся регулятор-

ная среда, растущая конкуренция, и т. д. Решение этих проблем неизбежно требует все большего количества и качества информации. Это, в свою очередь, влечет за собой необходимость в информационной грамотности сотрудников (либо в услугах компетентной фирмы, специализирующейся на коммерческой разведке).

Смартфоны, планшеты, сенсоры и беспроводные технологии — все это оказывает огромное влияние на *информационный ландшафт*, в котором прокладывают свой путь организации. Количество источников коммерческой информации будет расти по мере роста нашей собственной готовности использовать новые и инновационные каналы коммуникаций. Компания, которая *знает*, какими источниками следует пользоваться, и *умеет* их эксплуатировать, неизбежно получает конкурентное преимущество. Организациям необходимо работать над повышением своей информационной грамотности. Эти знания и умения — не приятный довесок ко всему остальному. Они абсолютно необходимы для самого выживания организации. Более того, от них зависит конкурентоспособность всего государства.

Какое будущее ждет отрасль коммерческой разведки? Учитывая нынешнее состояние экономики, я думаю, что крупные компании консолидируют рынок путем слияний и поглощений. При этом будут продолжать появляться все новые мелкие, нишевые фирмы, специализирующиеся на конкретных узких областях коммерческой разведки.

ИНДЕКС БЕЗОПАСНОСТИ: В чем заключается основное отличие разведки из открытых источников от традиционной разведывательной деятельности, которой занимаются в основном государственные секретные службы? Есть ли прецеденты, когда государственные службы — к примеру, аналитические отделы или даже сами разведслужбы — пытались передать в рамках аутсорсинга отдельные свои функции компаниям, специализирующимся на разведке по открытым источникам? Практикуется ли сотрудничество между такими компаниями и государственными службами на некоммерческой основе?

ПАЛЛАРИС: Обычно ответ на подобный вопрос звучит примерно так: разведка из открытых источников — это сбор данных из несекретных источников информации. В традиционной, или засекреченной, разведке используется более широкий спектр источников и методов получения нужной информации, включая агентурную работу, фотографии со спутников, и так далее.

На самом деле я не уверен, насколько такое определение было и остается правильным. Поясню: информация из открытых источников составляет 95% всей информации, которая необходима разведслужбам для обеспечения национальной безопасности и принятия политических решений. Почему это так? Потому, что добывать засекреченную информацию трудно и дорого. Ценность такой информации зачастую сомнительна, при этом она имеет свойство быстро устаревать. Конечно, это не значит, что такая информация бесполезна. Но ценность ее всегда является ограниченной.

Разведка из открытых источников является одним из ведущих направлений развития традиционных разведслужб. В откровенном разговоре любой профессионал в области разведки признает, что информация из открытых источников всегда являлась главной опорой любой компетентной разведслужбы. Во времена холодной войны советские разведчики значительную долю своего времени тратили именно на внимательное чтение газет, журналов, каталогов и тому подобных печатных источников в поисках информации, которая может оказаться полезной для агентуры. По имеющимся данным, результаты этой работы были очень впечатляющими.

Секретные службы собирают данные из всех возможных источников — но в очень многих случаях они полагаются прежде всего на информацию из открытых источников. Иными словами, в некоторых вопросах безопасности именно к такой открытой информации обращаются в первую очередь. А во всех остальных вопросах к ней обращаются в первую, последнюю и единственную очередь. Соответственно, умение работать с информаций из открытых источников — а также профессио-

нализм во всех остальных областях, относящихся к сбору информации и разведке — является залогом успешной разведывательной работы.

Дефицит профессионалов в данной области может объяснять тенденцию к аутсорсингу сбора информации — но это не единственное объяснение. За последние десять лет государственные органы начали рассматривать с точки зрения безопасности все до единого аспекты жизни страны — продовольственная безопасность, водная безопасность, энергетическая безопасность, экономическая безопасность, и т. д. Почему так происходит — тема для отдельного разговора. Но конечный результат очевиден: это постоянно растущая потребность в информации. Поясню: безопасность ведет к уверенности. Чем прочнее безопасность, тем больше уверенность в завтрашнем дне. И наоборот, отсутствие безопасности ведет к неуверенности и неопределенности. Чем выше степень неопределенности, тем больше нам нужно информации, чтобы эту неопределенность снять. Любое правительство работает в условиях большой неопределенности. Соответственно, продолжает расти его потребность в информации. Ни у одного правительства в мире нет достаточных ресурсов, чтобы полностью удовлетворить все свои потребности в информации — отсюда тенденция к аутсорсингу разведки и сбора информации.

Характерно, что большинство коммерческих компаний, которым госорганы передают некоторые свои функции в области сбора информации, работают исключительно с открытыми источниками. Отсюда следует, что если бы государственные служащие были лучше обучены работе по сбору информации из открытых источников, то расходы на аутсорсинг этих функций можно было бы значительно сократить.

Тем не менее, мне кажется, что рынок коммерческой разведки будет продолжать расти, хотя бы в силу того множества рисков и вызовов, с которым сталкиваются правительства.

ИНДЕКС БЕЗОПАСНОСТИ: Есть ли у вас планы развития, которые предполагают сотрудничество с компаниями (или даже государственными службами) из России, постсоветских стран или государств Восточной Европы? Есть ли планы прямой экспансии на этих рынках? Какие крупные национальные или региональные рынки за пределами Западной Европы кажутся наиболее привлекательными для компаний, специализирующихся на разведке по открытым источникам?

ПАЛЛАРИС: Пока что мы не занимались никакими совместными проектами за пределами Европы и Северной Америки. Однако мы готовы выслушать предложения, и каждое такое предложение мы рассмотрим индивидуально.

Будучи профессионалом в области образования, я особенно стремлюсь к сотрудничеству с университетами и бизнес-школами, чтобы помочь им обеспечить своих студентов теми знаниями и умениями, которые незаменимы в XXI в. Сюда входит умение собирать и анализировать информацию; обмениваться информацией; работать в условиях неопределенности и учитывать множество факторов; заниматься стратегическим планированием и прогнозированием; думать критически, креативно и концептуально, чтобы всегда быть хорошо приспособленным к быстро меняющейся деловой среде; а также уметь извлекать пользу из рисков и возможностей. Насколько можно судить, такие знания и умения сейчас в дефиците. В университетах такому учат редко, а на рабочем месте — практически вообще никогда. Мне такая ситуация кажется удивительной — ведь именно такие качества желают видеть в своих сотрудниках руководители компаний на протяжении вот уже двадцати лет.

Более того, я бы даже сказал, что нынешний экономический кризис во многом объясняется тем, что значительный процент европейской рабочей силы не имеет умений и навыков, необходимых для работы в экономике знаний. К примеру, средний офисный работник тратит до двух дней в неделю на безуспешные поиски информации. Подумайте, насколько более продуктивной стала бы их работа, если бы они на эти поиски тратили на 50 или на 80% меньше времени?

Нарастающая проблема кибершпионажа отражает эту динамику. В условиях нынешней экономики существует три способа получить необходимую для успешной конкуренции информацию. Можно инвестировать время и ресурсы в то, чтобы самостоятельно получить подробную картину своих рынков, клиентов и конкурентов. Можно эту работу поручить кому-то другому, в надежде, что подрядчик ее выполнит качественно. И, наконец, можно нанять хакера, чтобы он для вас крал любую информацию, которая ему подвернется под руку.

Только первый из этих трех подходов гарантирует получение дивидендов. Почему? Потому что те организации, которые учатся тщательным и этически безупречным образом собирать самостоятельно всю необходимую информацию, одновременно совершенствуют саму свою *способность учиться*. Именно способность учиться отличает успешные организации от неудачников. Красть чужие секреты легко — но вовсе не факт, что эти секреты пойдут на пользу вашей организации.

ИНДЕКС БЕЗОПАСНОСТИ: Насколько активно ваша компания использует для сбора информации социальные сети? Какие аналитические инструменты используются для обработки и анализа огромных массивов данных, полученных их социальных сетей и всего интернета?

ПАЛЛАРИС: Социальные сети и социальные СМИ сейчас являются очень актуальной темой для профессионалов в области как коммерческой разведки, так и национальной безопасности. Возможно, это объясняется тем, что профессионалы во всех аспектах разведки и сбора информации с очевидным запозданием осознали ценность и потенциал этих источников.

Чтобы понять эту ценность, нужно сперва понять человеческое поведение. Для людей характерно непреодолимое желание общаться. Общение — будь то с друзьями, семьей, или с миллионами незнакомых людей в интернете — является для нас некой валидацией нашего существования. Социальные сети удовлетворяют и усиливают наше стремление осознавать, что мы живы, и взаимодействовать с другими людьми. Это может звучать цинично, но на самом деле это вполне естественное для любого человека желание. Все это в равной степени относится и к организациям, которые состоят из отдельных людей.

Неизбежным образом эти отдельные люди делятся друг с другом информацией, которую, возможно, им стоило бы держать в секрете. Это информация о новых клиентах, о корпоративной стратегии своей компании, о провалах каких-то проектов, и так далее. Они при этом используют каналы, которые открыты для всех, в том числе и для профессионалов в области коммерческой разведки и сбора информации. Все, что нужно, чтобы получить такую информацию из социальных сетей — это хорошее знание источников информации и знание основ RSS/XML. Не обязательно даже добавлять организацию в свои *друзья* в *Facebook* или *Twitter,* чтобы узнать, о чем эта организация думает, чем она занимается и о чем говорит.

Профессионалы в области безопасности и правоохранительной деятельности также все больше осознают ценность социальных СМИ. Приведу лишь один пример: в этом году вышло несколько статей о том, как китайские блогеры, интересующиеся военной техникой, публикуют в своих блогах фото новейших китайских боевых самолетов и кораблей. Делают они это из соображений национальной гордости, в порыве искреннего энтузиазма. Но тем самым они также снабжают иностранные разведслужбы ценной информацией, на получение которой у тех могли бы уйти недели или месяцы, а также десятки тысяч долларов. Поэтому знание того, какие блоги представляют ценность, и как правильно проводить их мониторинг, становится очень важным.

Однако я не считаю, что социальные сети станут гигантским хранилищем данных, которым может воспользоваться любая желающая организация. Более того, я подозреваю, что в долгосрочной перспективе делать это будет все сложнее.

В любом случае, есть предел тому, что организации реально могут сделать со всей накопленной информацией. Есть, например, чисто практические ограничения на объем информации, который можно хранить. Есть и юридические ограничения: накопление огромного количества личных данных пользователей далеко не приветствуется законодательством, по крайней мере, в Европейском Союзе. Более того, ЕС стремится ввести такие правила, в соответствии с которыми личные данные пользователей, переданные социальным сетям, остаются собственностью самих пользователей. Время покажет, насколько успешной окажется эта инициатива. В любом случае, наиболее существенное ограничение связано тем, что сам объем данных, которые мы постоянно генерируем, огромен. Для обработки всех этих данных просто не хватит ни инструментов, ни технологий, ни людей.

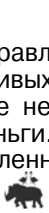
Конечно, многим из нас приятно думать, что правительство внимательно следит за всем, что мы сказали и написали в интернете. Если это действительно так, то я не завидую тем несчастным людям в секретных службах, которым все это приходится читать. Один из несомненных уроков *Арабской весны* состоит в следующем: если вы хотите, чтобы правительство просто накрыло с головой потоком информации, генерируйте как можно больше этой самой информации (причем желательно с использованием новых коммуникационных средств, которые власти еще не успели взять под контроль). Второй закон термодинамики отлично работает в политической практике — в частности, когда речь идет о свержении правящего режима.

ИНДЕКС БЕЗОПАСНОСТИ: Используете ли вы в своей работе новейшие аналитические инструменты, такие как *прогностический анализ*, которым, в частности, пользуется американская компания *Recorded Future*? Как Вы оцениваете потенциал и эффективность использования для прогностического анализа инструментов на основе так называемых *темпоральных аналитических процессоров*?

ПАЛЛАРИС: Я знаком со многими передовыми аналитическими инструментами; некоторые их них я тестировал по заказу наших клиентов. Кое-какие из них действительно очень эффективны. Есть и такие, которые не стоят тех денег, которые за них просят.

Каким бы ни был *калибр* этих инструментов, давайте не забывать, что все эти технологии все еще находятся на очень раннем этапе своего становления. Их способность выдавать точные прогнозы зависит от большого количества переменных, которые не имеют никакого отношения к самой технологии — в том числе от качества тех исходных данных, которые анализирует система, а также от умения аналитика максимально использовать возможности системы.

В любом случае, ни одна технология никогда не сможет делать на 100% точные прогнозы — так же, как этого не сможет сделать ни один человек. К примеру, ваша система может спрогнозировать, что В. В. Путин посетит Лондон во время Олимпийских игр. Она придет к такому выводу, *прочитав* пресс-релиз президентской службы, сообщающий о таком намерении главы государства. Система извлекает все относящиеся к делу данные (имена, даты, планы, географические пункты, и т. д.), сопоставляя их с уже известной информацией (то есть с информацией о том, что в Лондоне пройдут Олимпийские игры). Затем система выдает аналитику свой прогноз действий российского лидера. Если Путин действительно решит побывать на Олимпийских играх, то система окажется права. Если он решит не ехать в Лондон, а посмотреть дома телевизор, то система ошиблась. Это, конечно, очень примитивное описание того, как работают прогностические аналитические системы, но общая идея, надеюсь, вам понятна.

Несмотря на все это, я считаю, что данное направление имеет огромный потенциал, и что оно будет привлекать самых талантливых IT-специалистов всего мира. Наше желание знать или предвидеть будущее непреодолимо. За умение это делать организации готовы платить хорошие деньги. Однако сами по себе инструменты не являются панацеей от риска и определенности. Отдать анализ и принятие решений на откуп компьютеру не получится. 

Михаил Якушев

ИНТЕРНЕТ–2012 И МЕЖДУНАРОДНАЯ ПОЛИТИКА[1]

Начну статью с несколько необычного, лингвистического, а точнее орфографического, аспекта проблемы. По сути, его можно выразить простым вопросом: как в русском тексте правильно писать эквивалент всем известного слова *Internet*?

Исторически, начиная с 1990-х гг., существовало несколько способов написания этого слова: «*Internet*», *Internet*, *сеть Internet* (без транслитерации), «*Интернет*», *ИНТЕРНЕТ*, «*сеть Интернет*», *Интернет* (без кавычек, как несклоняемое существительное женского рода либо как существительное мужского рода, склоняемое аналогично слову *Центризбирком*) и, наконец, *интернет* со строчной буквы, склоняемое по правилам существительных мужского рода, аналогично слову *телефон*. Экзотические варианты типа *Интерсеть* или *междусеть* не выдержали испытания временем и остались скорее разовыми *орфографическими курьезами*.

В настоящее время все чаще проявляется тенденция написания слова интернет со строчной буквы, что знаменует переход этого понятия из категории имен собственных (как обозначения названия некоторой международной компьютерной сети) в категорию имен нарицательных — как обозначения инфраструктуры, обеспечивающей определенную технологию обмена информацией. Устоявшегося, нормативного закрепления этой точки зрения пока нет — хотя в современных условиях фиксация литературной орфографической нормы заметно отстает от жизни[2]. Высказывается также мнение, что вариативность написания «интернет–Интернет» может иметь смыслоразличительную функцию, однако эта точка зрения слишком трудна для восприятия неспециалистом в области компьютерных систем. Кроме того, уже практически повсеместно слово *интернет* пишется со строчной буквы во всех случаях, когда оно составляет часть сложных слов, например, в таких терминах, как *интернет-сервер*, *интернет-сайт*, *интернет-услуги*.

Конечно, соответствующая дискуссия не может не иметь определенного политического подтекста, впрочем, малопонятного, скажем, для англоязычной аудитории. Переход на написание *интернет* окончательно ликвидирует возможность отношения к этой международной информационной сети как к некоему объекту регулирования, который а) кому-то *принадлежит*, б) носит в этой связи присвоенное фактическим или формальным владельцем имя или название, в) сосуществует с некими *иными* объектами, сходными с ним по принципам функционирования и развития. В частности, основной массив российского законодательства избегает употребления слова *интернет*, предпочитая подменять его эвфемизмом *информационно-коммуникационная сеть*[3], хотя в последнее время все чаще *название* этой информационно-коммуникационной сети прямо вводится в текст федеральных законов.

В то же время последняя из сетей, которая могла бы быть названа информационно-коммуникационной, хотя и не международной: знаменитая французская *Minitel,* — прекратила свое существование 1 июля 2012 г.[4]. Таким образом, сегодня интернет, что бы мы не под ним не понимали, уже не имеет каких-либо *конкурентов* в части технологий глобального распространения информации с использованием компьютерных и мобильных абонентских устройств, поэтому уместно во всех случаях отказаться от графического выделения *особости* интернета как глобальной инфраструктуры распространения информации в электронном виде и окончательно перейти на написание соответствующего термина со строчной буквы, что и предлагается сделать дальше повсеместно.

Вопросы, связанные с регулированием инфраструктуры интернета уже становились предметом заинтересованного анализа[5], настало время отметить основные события, произошедшие в интернете к осени 2012 г. и проверить обоснованность и осуществимость сделанных прежде выводов и предположений. Таким образом, цель настоящей статьи — дать читателю обобщенное представление о текущей ситуации в управлении интернетом на глобальном уровне и о возникающих при этом политических и геополитических проблемах.

УПРАВЛЕНИЕ ИНТЕРНЕТОМ: ТЕОРИЯ И ТЕРМИНОЛОГИЯ

К середине 2012 г. общепринятых определений понятия *интернет*, а также понятия *управление интернетом* так и не появилось. По-прежнему актуальны выводы *Рабочей группы по управлению интернетом*, сформированной в 2004 г. Генеральным секретарем ООН из числа экспертов более чем из 40 стран, большинство из которых продолжает активную деятельность в области изучения разных аспектов развития Сети. Напомним, что результаты ее работы вкратце могут быть представлены следующим образом:

1) понятие *интернет* уже настолько общеизвестно и интуитивно понятно, что какие-либо его дополнительные определения просто не нужны;

2) для понятия *управление интернетом* как процесса выработки нормативных правил функционирования и развития Сети ключевым является взаимодействие трех групп *заинтересованных участников*[6]: государственных органов, бизнеса и институтов гражданского общества, к которым относят в первую очередь неправительственные и некоммерческие организации, включающие объединения пользователей интернета. При этом зачастую к кругу этих заинтересованных участников стали добавлять представителей науки и образования (*Academia*);

3) в качестве общемировой площадки для продолжения дискуссий по этому вопросу учрежден глобальный Форум по управлению интернетом [Internet Governance Forum][7]. Осенью 2012 г. очередной, уже седьмой Форум запланирован в столице Азербайджана городе Баку.

Не утихают международные дискуссии, связанные по вопросу управления интернетом в части двух различных подходов к указанной проблематике. Так называемый *узкий* подход подразумевал, что управление интернетом сводится лишь к установлению правил распределения сетевого адресного пространства как на международном уровне, так и в рамках национальных государств: к порядку создания и функционирования *доменных зон,* правил использования операторами связи *сетевых (IP) адресов* и т. д. Противоположный, так называемый *широкий* подход относил к управлению интернетом намного более широкий круг вопросов гуманитарного, политического и экономического характера — от проблем многоязычия в интернете, обеспечения культурного разнообразия и борьбы с использованием Сети в противоправных целях до достаточно спорных предложений о пересмотре глобальной экономической модели управления телекоммуникационной инфраструктуры в пользу наименее развитых стран мира. Исходя

из принципа *многостороннего участия* в управлении интернетом *(государство + бизнес + гражданское общество)* представляется, что оптимальной была бы комбинация обоих подходов с более четким определением того, на каком *уровне* (межгосударственном, национальном) и с использованием каких средств (правовых, технических, организационных) следует решать те или иные вопросы развития Сети.

В последнее время наблюдается расхождение подходов в таком важном аспекте управления интернетом, как безопасность его использования. Российская Федерация наряду с несколькими соседними государствами предлагает исходить из более широкого понятия *международной информационной безопасности* (МИБ), включающего все аспекты взаимодействия государств в информационном пространстве[8]. При этом Соединенные Штаты и большинство их союзников предпочитают по-прежнему говорить о *кибербезопасности,* или о *безопасности киберпространства*[9], сводя соответствующую проблематику в основном к регламентации функционирования компьютерных и иных информационных систем.

Совокупность проблем управления интернетом по-прежнему базируется на *основных принципах*, к числу которых следует отнести:

- порядок маршрутизации информационных (содержательных) и необходимых технических сообщений между узлами интернета. Иначе говоря, такого рода сообщения должны доходить от отправителя до адресата с минимальными затратами и желательно без каких-либо потерь данных должен быть единым для всей Сети, иначе будет невозможно обеспечить *связность* различных (территориально или технологически распределенных) компонентов интернета;
- порядок преобразования сетевых IP-адресов в уникальные доменные имена, без соблюдения которого невозможна однозначная адресация сетевых ресурсов.

Все эти базовые принципы напрямую вытекают из основной идеи создания в конце 1960-х гг. информационной сети, позволяющей сохранить устойчивость и хотя бы частичную функциональность в условиях массированного ракетно-ядерного удара СССР по командным центрам стратегических сил США[10].

В силу отмеченных особенностей архитектуры интернета как информационной сети, различных исторических, технологических и политических причин ключевыми факторами, влияющими на регулирование деятельности по распределению доменных имен и IP-адресов, являются:

- трансграничный характер отношений по поводу обеспечения функционирования интернета — эта информационная сеть существует и развивается независимо от национальных (государственных) границ;
- высокая роль стандартов и протоколов, соответственно, технического регулирования и саморегулирования;
- исторически обусловленное техническое и экономическое лидерство США в сфере развития сети интернет. Нельзя не отметить, однако, что указанное *лидерство,* вне всяких сомнений, перестает быть настолько очевидным, как это казалось еще несколько лет назад, и, что более важно, оно последовательно и активно отвергается все большим числом других стран.

Указанные факторы привели к возникновению современной системы управления базовыми функциями сети интернет, которая практически не претерпела фундаментальных изменений с начала века. Общее руководство процессами развития Сети по-прежнему осуществляет некоммерческая организация *Общество интернета* [Internet Society, ISOC][11]*,* с офисами в штате Вирджиния (США) и в Женеве. Ее

инженерное подразделение IETF *(Internet Engineering Task Force)*[12] разрабатывает и принимает стандартизированные «заявки на рекомендации» (RFC)[13], в соответствии с которыми создается программное обеспечение и осуществляется связность между составными частями интернета.

Фактически же основную роль в обеспечении единства адресного пространства и уникальности доменных имен играет *Корпорация интернета по присвоению имен и адресов,* более известная по английской аббревиатуре ее названия — ICANN *(Internet Corporation for Assigned Names and Numbers)*[14]*.* Более подробно об ICANN будет сказано ниже. Обе организации возникли при активной поддержке правительства США и впоследствии наладили достаточно эффективное взаимодействие с большинством организаций и государственных органов, заинтересованных в регулировании и/или саморегулировании интернета в других странах.

Помимо указанных организаций, в процессах управления интернетом участвуют:

- правительство США, в частности его Департамент торговли, передавший ICANN полномочия в области регистрации распределения сетевого адресного пространства;
- международные организации (в том числе специализированные учреждения ООН) — Международный союз электросвязи [ITU], Международная организация по стандартизации [ISO], которые разрабатывают и принимают стандарты и организационно-технические нормы, причем часть из них используется при функционирования интернета, преимущественно в области телекоммуникационной инфраструктуры. Отдельные аспекты регулирования интернета также рассматриваются Всемирной организацией интеллектуальной собственности (WIPO) и ЮНЕСКО;
- региональные регистраторы (RIR) — некоммерческие организации, получающие блоки сетевых IP-адресов от ICANN на основании соглашения и распределяющие их в своем регионе на основании заявок от провайдеров. Одним из пяти региональных регистраторов является Центр координации региональной интернет-регистрации [RIPE NCC][15], осуществляющий деятельность для Европы, в том числе для Российской Федерации;
- регистратуры доменных имен первого уровня — организации, поддерживающие базы данных доменов первого уровня и осуществляющие контроль уникальности доменных имен. В Российской Федерации такой организацией является автономная некоммерческая организация *Координационный центр национального домена сети интернет (КЦ НДСИ)*[16];
- регистраторы доменных имен — организации, осуществляющие регистрацию доменных имен на основании соглашений с пользователями, с одной стороны, и национальной Регистратурой (или ICANN) — с другой. В России аккредитовано около 30 компаний-регистраторов;
- операторы услуг доступа к интернету (часто и неточно именуемые *провайдеры)* — многочисленные, преимущественно коммерческие организации, организующие доступ в интернет конечных пользователей;
- администраторы серверов (ресурсов) интернета — пользователи (как организации, так и граждане), получившие постоянные зарегистрированные адреса и доменные имена, размещающие по полученным адресам информационные ресурсы и (или) оказывающие информационные услуги;
- пользователи — лица, на основании договоров с операторами услуг получающие доступ к ресурсам интернета. Общественные объединения пользователей Сети как на глобальном уровне, так и в отдельных странах

достаточно активно участвуют в процессах выработки решений, относящихся к управлению интернетом;

- органы власти различных государств, принимающие законодательные и иные правовые акты, регулирующие использование интернета в соответствующих национальных юрисдикциях.

ГЛОБАЛЬНАЯ СИСТЕМА ДОМЕННЫХ ИМЕН: ПРИНЦИПЫ РАБОТЫ

Центральное место в функционировании интернета занимают отношения в области обеспечения единства глобальной сети и единой адресации, системы имен и нумерации портов, стандартов и протоколов, которые делают Сеть одинаково доступна в любой ее точке. Одним из центральных элементов в рамках этой сложной системы отношений являются вопросы обеспечения работы доменных имен. Доменное имя является вторичным ресурсом, созданным для удобства обращения к сайтам, оно представляет условное наименование (например, *www.pircenter.org* для московского ПИР-Центра), однозначно соответствующее определенному IP-адресу.

Для удобства использования всех нынешних и, вероятно, будущих интернет-услуг используется единая технология доменного пространства, упорядочивающая все информационные ресурсы интернета, позволяющая их быстро находить и получать к ним доступ. В отличие от IP-адресов, формирующих одноуровневую структуру взаимодействия из множества компьютерных узлов Сети, которые соединяются линиями связи, система доменных имен представляет собой иерархическую древовидную структуру, разбивающую все множество узлов интернета на отдельные *сегменты* — домены. Функционирование системы доменных имен в масштабах всей Сети обеспечивает распределенная система, состоящая из многих серверов с собственной иерархией.

Особое значение для функционирования Сети имеют *домены первого уровня.* До последнего времени они традиционно подразделялись на домены *географические (country-code top-level domains)* и *общего назначения (generic top-level domains).* Их обозначение представляет собой крайне правую часть сетевого адреса, отделенную от других частей (доменных имен второго и последующих уровней) точкой: например, *.ru* для доменной зоны Российской Федерации и *.aero* для доменной зоны общего назначения, используемой организациями гражданской авиации. Правила создания доменных имен позволяют фактически не ограничивать многообразие всех возможных доменов, поскольку число возможных комбинаций букв и символов в их именах существенно превышает лексический запас любого языка. Вследствие этого ключевое значение приобретает тот, кто вправе является администратором домена и какие правила существуют для регистрации в нем доменных имен.

Из существовавших до последнего времени порядка 20 доменов общего назначения *(.com, .org, .net* и др.) большинство администрируются американскими коммерческими фирмами либо, если речь идет о доменах типа *.gov* или *.mil,* соответствующими уполномоченными организациями. Именно в доменных зонах общего пользования (а вовсе не в географической зоне *.us)* регистрируется подавляющее большинство американских пользователей Сети.

Что же касается географических (или *страновых*) доменов, то соответствующие *географические* принципы распределения интернет-адресов несколько отличаются от привычной нам политической географии мира. ICANN традиционно проявляет максимальную гибкость в решении вопросов создания новых доменов и ликвидации старых. При этом на территории одной страны может существовать одновременно два домена (так, для Великобритании — реально используемый *.uk* и практически неработоспособный *.gb;* в России действует национальный домен *.ru* и еще *советский* домен *.su).* А в случае радикальных изменений политической

карты в том или ином регионе, как правило, проходит некоторое время, пока новый субъект международного права получит свой домен первого уровня. Основой для принятия соответствующих решений является таблица международного стандарта Международной организации по стандартизации (ИСО) *3166-1*[17], рекомендующая двухбуквенные коды стран, которые и используются при назначении новых (или для отмены уже *неактуальных)* национальных доменных имен.

Этот международный стандарт (утверждаемый ИСО) позволяет формально избегать каких-либо *геополитических конфликтов* в интернете при попытках отделения тех или иных территорий от государств, признаваемых субъектами международного права. Именно поэтому для Косово действует сербский домен *.rs* (хотя большинство косовских сайтов размещается в иных доменных зонах), а для Черногории был выделен новый домен *.me.* Однако это не снимает напряженности между ICANN и правительством Китайской Народной Республики по поводу существующего домена *.tw,* используемого на Тайване, официально рассматриваемого КНР как провинции, составной части своей территории.

Географические домены, таким образом, могут появляться и исчезать. Так, были аннулированы домены *.dd* (для ГДР),.*cs* (для Чехословакии) и *.yu* (для Югославии), а домены *.tp* и *.zr* уступили новым доменам в связи с переименованием соответственно Восточного Тимора и Заира (имеются в виду домен *.tl* для Тимора-Леште и *.cd* для Демократической Республики Конго).

В настоящее время, в соответствии с указанным стандартом ИСО *3166-1,* определено более 200 географических доменных зон первого уровня, из которых подавляющее большинство является действующими доменами (в которых осуществляется регистрация доменных имен второго уровня). Отмечены, однако, случаи появления доменов без их фактического администрирования (например, для Западной Сахары, для недолго просуществовавшего государственного образования под названием Сербия и Черногория, а также для некоторых заморских территорий Франции). Существуют также географические домены, фактически не используемые по тем или иным причинам. Одним из примеров служит упоминавшийся формально принадлежащий Великобритании домен *.gb,* регистрация в котором не производится, в то время как фактической британской географической зоной является домен *.uk.* Также стоит упомянуть существующие с нарушением формального принципа соблюдения стандарта ИСО *3166-1,* например, используемый в России домен Советского Союза *.su.*

В целом случаи появления и (не)использования *нестандартных* доменов в основном связаны с геополитическими изменениями на карте мира, причем реальные действия ICANN по корректировке перечня существующих доменов направлены на обеспечение максимальной стабильности уже существующих доменных зон и поддержки зарегистрированных в них сайтов.

Подобно тому, как не существует одинаковых политических систем даже в странах со сходным географическим положением и общностью исторического и социально-экономического развития, не существует и одинаковых моделей администрирования национальных (географических) доменных зон. Кроме того, следует отметить, что сама по себе выбранная модель администрирования национального домена не влияет непосредственно на количественные показатели развития домена (число зарегистрированных доменов второго уровня, динамика роста и т. п.). Здесь в первую очередь должны приниматься во внимание иные факторы: степень проникновения интернета (число пользователей Сети по отношению к общему числу жителей страны), степень экономического развития страны, общая и компьютерная грамотность населения, государственная политика в отношении интернета и т. д. Тем не менее используемые модели администрирования национальных доменов можно свести к нескольким типовым схемам:

- непосредственное управление национальным доменом уполномоченным органом власти соответствующего государства (типичные примеры — Китай, Аргентина);
- управление доменом со стороны частной (коммерческой) компании, которая, помимо администрирования домена первого уровня, может оказывать услуги по регистрации доменных имен второго уровня; здесь также должны рассматриваться профессиональные (саморегулируемые) объединения организаций-регистраторов (типичные примеры — Великобритания, Австрия, Украина);
- управление доменом со стороны *компромиссной* некоммерческой (либо образовательной или научной) организации, уполномоченной на это местным интернет-сообществом и (или) соответствующей государственной инстанцией (примеры — Литва, Кипр, сюда же следует отнести российский домен *.ru*);
- своеобразный *вырожденный* случай администрирования национального домена иностранной коммерческой компанией по договору с правительством соответствующей страны. Наиболее типичным примером такого рода является домен *.tv* тихоокеанского островного государства Тувалу.

Правила регистрации доменных имен в национальных доменах существенно различаются. Есть домены с многомиллионными регистрациями, есть небольшие домены, число регистраций в которых ограничивается несколькими десятками или сотнями. Однако некоторые лингвистические особенности, связанные со страновыми доменами, которые оказываются омонимичны некоторым аббревиатурам или значащим иноязычным словам, существенно *искажают* статистику регистраций в отдельных доменных зонах.

В качестве примера приведем такую специфическую модель администрирования национального домена, как домен первого уровня уже упоминавшейся Республике Тувалу, — одной из стран мира, практически лишенных природных ресурсов, чье немногочисленное население проживает в отдаленной части Тихого океана. Национальный домен Тувалу *(.tv)* является удобным *суффиксом* для наименований сетевых ресурсов, связанных с телевидением, поскольку *TV* — общепринятое в мире сокращение терминов, связанных с телевещанием. Указанная ситуация послужила причиной того, что число регистраций в соответствующем домене несопоставимо *велико* по сравнению с потенциальным числом пользователей интернета в Тувалу и степенью экономического развития этой страны.

Администратором домена с 1996 г. (по долгосрочному контракту с правительством страны) является дочернее подразделение американской компании *VeriSign — dotTV Corporation*. Фиксированные отчисления от регистрации доменов в этой зоне, предназначающиеся правительству Республики Тувалу (и достигающие нескольких миллионов долларов США в год), составляют существенную часть доходов государственного бюджета страны. Таким образом, фактически национальный домен управляется зарубежным юридическим лицом (хотя правительство Тувалу имеет некоторую долю в уставном капитале корпорации *dotTV),* исключительно в коммерческих целях. В этой связи, например, вообще не проводится каких-либо проверок того, в какой стране находится (проживает) заявитель и какие цели он преследует для регистрации доменов в *телевизионной* доменной зоне.

Аналогичная ситуация складывается для тихоокеанского же острова Ниуэ. Его домен *.nu* в скандинавских языках означает *сейчас,* а во французском — *обнаженный.* Этим и объясняется относительная популярность островного домена для организаций, занимающихся маркетинговыми акциями в Скандинавии и распространением эротической продукции — повсеместно. Еще два примера: весьма привлекательный для радиостанций и радиовещательных корпораций домен *.fm,* принадлежащий Микронезии (совпадающий с общепринятым обо-

значением УКВ-диапазона вещания), и новый конголезский домен *.cd* (совпадающий с обозначением компакт-дисков и поэтому привлекательный для компаний звукозаписи).

В перспективе можно ожидать *всплеска* популярности и доменов, подобных туркменскому *.tm* (совпадает с общепринятым обозначением *товарный знак),* активное продвижение которых ограничивается в настоящий момент лишь весьма жесткими правилами регистрации доменов второго уровня в соответствующих зонах. Однако это вызывает и вопросы, насколько *далеко* можно зайти в предоставлении прав использования национальных доменов иностранными лицами, насколько деятельность таких лиц подлежит контролю, а данные о них — сбору и регистрации.

РАСШИРЕНИЕ ДОМЕННОГО ПРОСТРАНСТВА: ТЕНДЕНЦИИ И ПРОБЛЕМЫ

Однако главные, поистине *революционные* изменения в глобальной системе доменных имен в течение последних лет происходят в связи со введением новых доменных зон, которое окончательно размывает *границу* между географическими доменами и доменами общего назначения.

Еще в 2005 г. ICANN одобрила введение новых доменов первого уровня, из которых часть можно было бы отнести к категории *отраслевых* (таких как *.travel, .mobi* или *.tel),* домен *.asia* — к наднациональным, а вот домен.*cat* стал первым доменом, выделенным не государству и не государственному объединению (подобно домену Европейского Союза *.eu),* а фактически этнической или языковой общности — фонду развития каталонского языка. К слову, если бы в домен *.cat* была бы допущена свободная регистрация, не связанная с обязательной *привязкой* администраторов к Каталонии, то, скорее всего, этот домен превратился бы в основной интернет-ресурс любителей кошек и рекламы продукции для домашних питомцев.

С весны 2012 г. реализуется решение о возможности создания практически неограниченного числа доменов первого уровня по запросу заинтересованных лиц. Уже в первые месяцы приема заявок на *свободную* регистрацию доменов первого уровня (подобных *.google* или *.pircenter*) число таких заявок составило порядка полутора тысяч, в том числе из России, такие как *.дети, .католик, .ком, .москва*, *.онлайн, .орг, .рус* и *.сайт*[18]. В настоящее время проводится работа по подготовке запуска и делегированию первых таких доменов, и уже возникли первые, причем достаточно серьезные, конфликты по поводу самого существования отдельных названий, предлагаемых для использования в качестве доменов первого уровня. Так, Саудовская Аравия выдвинула претензии по поводу возможности запуска доменов *.gay, .vodka, .sex* и некоторых других[19]. В любом случае полномасштабный запуск проекта «новых доменов общего пользования» можно ожидать не раньше чем через год-полтора, то есть примерно к концу 2013 г.

Несколько лет назад также было принято решение о создании так называемых интернационализированных доменов первого уровня [Internationalized Domain Names], для обеспечения более удобного доступа к Сети пользователям, чьи языки построены на иной, по сравнению с латиницей, графической основе.

Идея о возможности создания сетевой адресации с использованием символов, отсутствующих в латинском алфавите, стала особенно популярной в 1990-е гг., когда интернет приобретал миллионы новых пользователей в бывших республиках СССР, арабских странах, Индии и Китае, в других странах, где государственные языке базируются на графических основах, отличных от латиницы. Достаточно быстро появились *временные* технические решения, когда хотя бы для части пользователей национальных доменных зон можно было набирать левую часть адреса символами национального алфавита (например, китайскими иероглифами), а правую — по-прежнему указывать в стандартном виде — например,*.cn* для китайского

домена. При этом происходила автоматическая замена иероглифов в IP-адреса, позволяющая однозначно идентифицировать запрашиваемый сетевой ресурс.

Однако такое временное решение, которое, кстати, было подготовлено и в отношении кириллицы, но не было реализовано в России, имело существенные недостатки. Во-первых, сетевой адрес получался написан двумя разными алфавитами. Во-вторых, все подобного рода решения не были стандартизированы на глобальном уровне, а следовательно, за пределами соответствующей доменной зоны адреса либо отражались некорректно, либо вообще не обеспечивали гарантированный доступ к сетевому ресурсу. Была начата работа по созданию единых стандартов представления *интернационализированных* доменных имен для большинства используемых в мире нелатинских алфавитов, таких как кириллица, греческий, грузинский, армянский алфавиты, арабское письмо, иврит, индийские алфавиты, китайская и японская иероглифика, корейская система письма и т. д.

В результате во время четвертого Форума по управлению интернетом в египетском Шарм-эль-Шейхе (2009 г.) сразу несколько стран подали заявки на регистрацию соответствующих доменных зон. В частности, заявки были направлены на арабоязычные доменные зоны для Египта и Саудовской Аравии, также поступила заявка Китайской Народной Республики на соответствующий домен на китайском языке. Большинство заявок было удовлетворено, и первые нелатинские доменные зоны были запущены для всеобщего использования во второй половине 2010 г.

Во-первых, казались небезосновательными опасения некоторых пользователей Сети, что введением *национальных* доменных зон предпринимается попытка *фрагментации* ныне единого интернета, препятствующая свободному обмену информацией между различными географическими *сегментами.* Действительно, осуществлять фильтрацию интернет-трафика, исходящего из *нечитаемых* доменных зон, намного проще, чем анализ содержимого самих сайтов, на которых размещена соответствующая информация. Более того, пользователям интернета в других странах, у которых отсутствует возможность набора нелатинских символов с клавиатуры их компьютеров, практически будет невозможно получить доступ к сайтам в *иноязычных* доменных зонах. Впрочем, все эти вопросы могут быть решены с помощью автоматической переадресации между сайтами в разных доменных зонах и правильно выстроенной системы взаимных ссылок.

Во-вторых, и это особо характерно для таких стран, как Россия, с появлением *национальных* доменных зон интернет мог бы разделиться на *глобальный,* «нормальный во всех отношениях», и *местный,* «второго сорта», по аналогии с продукцией *отечественного автопрома*. Конечно, эти опасения, к счастью, оказались безосновательными — обе национальные доменные зоны развиваются совместно, без какого-либо *конфликта* между ними.

Отмеченные вопросы во многом носили *психологический* характер. Но есть и безусловные проблемы, порождаемые все усложняющейся структурой интернет-сервисов, в том числе в связи с введением новых доменных зон. Так, к сожалению, может осложниться борьба с противоправными деяниями в Сети, в частности с размещением в интернете информации антиобщественного содержания (т. е. запрещенной к распространению) или совершением мошеннических действий. В самом деле, если для *обычных* доменов и сайтов, использующих английский язык (латиницу) для идентификации их администраторов существуют достаточно простые алгоритмы и технологические средства, то в случае размещения, скажем, сайта с призывами к совершению террористических актов (написанными, конечно, по-русски), в амхарской, бирманской или сингальской зонах Сети поиск злоумышленника может быть существенно осложнен по очевидным причинам.

Кроме того, есть проблемы и с собственно *интернационализированными* доменами. Так, в соответствии с принятыми стандартами IDN хотя бы один символ в таком

домене должен обязательно не совпадать ни с одним из символов латинского алфавита. И если для арабских символов это правило соблюдается легко, то для кириллических сокращений это уже не так очевидно. Скажем, именно поэтому невозможен кириллический домен *.ру,* совпадающий омографически с доменом Парагвая *.ру.* Сокращение названия нашей страны (РФ) достаточно легко может быть преобразовано в домен *.рф,* поскольку графема *ф* отсутствует в латинском алфавите). А для Украины, в названии которой *все* кириллические буквы имеют графические аналоги в латинице, подобрать соответствующее доменное сокращение оказалось невозможно. В результате было принято решение остановиться на трех-, а не двухбуквенном сочетании *.укр*.

Есть проблемы и с названиями суверенных государств, которые оспариваются соседями. Наиболее известен греко-македонский спор о названии государства со столицей в Скопье, а также диспут по поводу отображения символов в адресной строке, связанный с особенностями арабского языка, в котором буквы пишутся справа налево, а цифры — слева направо. При этом возникает также вопрос, почему бы сразу не решить проблему и с кириллическими доменами для тех стран, точнее этнокультурных групп, в которых существенная часть населения владеет соответствующими языками и желала бы использовать более удобный для нее способ адресации в интернете. Речь, в частности, идет о кириллических доменах типа *.ста, .фрг,* возможно даже *.лондон* или *.мальорка.* Принципиальных технологических запретов для такого решения нет.

Реальная же практика создания и функционирования кириллического домена *.рф*, как и других нелатинских доменных имен первого уровня, показала, что принципиальных изменений на рынке регистрации доменов все же не произошло. В первый год (2010–2011 гг.) существования российского кириллического домена число регистраций в нем едва не достигло одного миллиона, и он превратился в один из наиболее быстро растущих доменов в мире. При этом, однако, не наблюдалось и сокращения числа регистраций в *традиционном* домене *.ru* (оно, кстати говоря, к концу 2012 г. превысит уже четыре миллиона доменных имен второго уровня. В то же время не исключено, что спрос на домены в кириллической зоне был несколько ажиотажным и необоснованным, вследствие чего значительная часть доменов в кириллической зоне так и была делегирована, то есть на указанных доменных адресах не появилось самостоятельных сайтов, и в настоящий момент число регистраций стабилизировалось примерно в районе 800 тыс. Ожидается, однако, что с появлением новых негеографических доменов число регистраций в традиционных и интернационализированных доменных зонах может несколько сократиться.

Развитие интернета в ближайшие годы поставит перед нами еще немало увлекательных задач. Обозначенные примеры, хотя и относятся к сравнительно небольшому по значимости кругу вопросов функционирования интернета, позволяют указать на одну из ключевых политических проблем управления Сетью: кто и на каких основаниях вправе принимать фундаментальные решения в отношении интернета. Поскольку, даже будучи формально *технологическими* по сути, такие решения всегда имеют далеко идущие социальные, юридические, экономические и, следовательно, политические последствия.

КОРПОРАЦИЯ ICANN: БОЛЬШАЯ ПОЛИТИКА НЕПОЛИТИЧЕСКОЙ ОРГАНИЗАЦИИ

Как уже отмечалось, ключевую роль в *управлении интернетом* — в части администрирования системы адресов и доменных имен — играет организация ICANN, зарегистрированная в американском штате Калифорния как «некоммерческая корпорация, созданная для общественной пользы». С 2009 по 2012 г. президентом ICANN был Род Бекстром (гражданин США, в прошлом — руководитель *Национального центра по кибербезопасности).* Штаб-квартира ICANN расположена в районе Лос-Анджелеса, вспомогательные офисы находятся еще в четырех горо-

дах США, Бельгии и Австралии. В общей сложности в офисах ICANN работает примерно 130 постоянных сотрудников[20].

Основой для функционирования ICANN в качестве организации, уполномоченной на администрирование в глобальном масштабе системы доменных имен, являлся Меморандум о понимании между ICANN и Департаментом торговли США (иногда также именовавшийся Соглашением о совместных проектах). Именно указанный Меморандум рассматривался как подтверждение *американского влияния* на управление системы доменных имен в глобальном масштабе. Однако следует иметь в виду, что само существование Меморандума было обусловлено стремлением Министерства торговли США прекратить какие-либо формальные связи между системой управления доменными именами и Администрацией США по окончании переходного периода, который должен был истечь в 2000 г. Декларировались, в частности, такие цели передачи функций администрирования ICANN, как развитие свободной конкуренции и интернационализация управления системы доменных имен.

Как показывает практика существования ICANN, в целом организация достаточно успешно справлялась с реализацией всех отмеченных выше функций, несмотря на наблюдавшиеся (особенно в 2012 г.) технические сбои в отладке системы регистрации новых доменов и участившейся критике со стороны ряда государств по поводу того, какие решения принимались органами ICANN и в какие сроки они были реализованы. Самым известным подобного рода конфликтом, на несколько лет прервавшим взаимодействие между ICANN и Китайской Народной Республикой, был спор об упоминавшемся выше тайваньском домене *.tw*. Вообще говоря, корпорация крайне неохотно идет на какие-либо радикальные решения, если при этом возможна негативная реакция хотя бы небольшой части государств или интернет-сообщества.

Так, если по тайваньскому домену зафиксирован *статус-кво* исходя из принципов соответствия таблицы ISO 3166-1, то запуск специализированной доменной зоны *.xxx*, предназначенной для размещения порнографических материалов, отменялся из-за противодействия целого ряда межправительственных организаций и ряда стран еще на этапе предварительных обсуждений и лишь впоследствии был вновь разрешен. А вот домен *.su*, продолжающий достаточно активно развиваться преимущественно в России, несмотря на исчезновение титульного государства (СССР), не был исключен ICANN из списка действующих доменных зон из-за достаточно большого числа уже проведенных в нем регистраций (в основном научных и образовательных учреждений).

Часть стран продолжают видеть в ICANN проводника американской модели управления интернетом, с одной стороны, основанной на принципе отказа от контроля за контентом в Сети, а с другой — все чаще предлагающей государственный контроль доступа к тем или иным сетевым ресурсам. Правозащитники упрекают ICANN в отказе от последовательной защиты свободы распространения информации. Справедливости ради, однако, следует отметить, что такой задачи перед этой организацией никто и не ставил. Многие эксперты считают механизм принятия решений в Корпорации чрезмерно усложненным, медленным и недостаточно прозрачным, а следовательно, малоэффективным в современных условиях.

Следует отметить, что в последнее время активность России по *интернационализации управления интернетом* в части изменения полномочий ICANN резко усилилась. В преддверии Всемирной конференции по международной электросвязи МСЭ в Дубаи, намеченной на 3–14 декабря 2012 г., ожидается, что в рамках группы БРИКС будут сформулированы новые предложения по изменению *баланса сил* по основным вопросам управления интернетом с возможной передачей большей части соответствующих полномочий Международному союзу электросвязи (МСЭ). При этом такие страны, как Бразилия, Индия и Южная Африка, готовы к некоему *промежуточному*, компромиссному варианту, при котором противостояние меж-

Пал ***Дунай (Венгрия)****, руководитель программы по международной безопасности Женевского центра политики безопасности — по электронной почте из Будапешта:* Сегодня многие на Западе, и в частности в США, озабочены предстоящей Всемирной конференцией Международного союза электросвязи (МСЭ) в Дубаи, намеченной на декабрь 2012 г. Некоторые эксперты и дипломаты боятся, что МСЭ ищет возможность усилить свое влияние и контроль над ключевыми элементами интернета. Ситуация усугубляется тем, что ее зачастую неверно понимают, так что составить четкую картину проблемы совсем не просто. В преддверии саммита группы правительственных экспертов МСЭ снова проведут серию встреч, для того чтобы обсудить вопросы стандартов и определений, связанных с функционированием интернета. Эти встречи станут продолжением предыдущих попыток согласовать терминологию, которая не будет вызывать противоречий между разными государствами.

ду ICANN и МСЭ может быть разрешено в пользу вновь создаваемой международной организации или специализированного учреждения ООН.

Очевидно, пока подобные предложения не будут поддержаны сколько-нибудь значимым числом государств, не говоря уже об организациях бизнеса или сетевого сообщества. Именно отсутствие серьезных проблем в администрировании глобальной системы интернет-адресов, несмотря на все сопутствующие при этом, хотя и вполне разрешимые со временем проблемы, позволяют придерживаться известного принципа *зачем чинить то, что не сломано*. Также не всегда продуктивной можно считать излишнюю политизацию данного процесса, вследствие которой даже за внешне разумными и обоснованными предложениями технического плана очень многие видят «закамуфлированные» идеи по установлению системы жесткой цензуры за всеми происходящими интернете процессами по образцу КНР.

ПАРАДОКСЫ РАЗВИТИЯ ГЛОБАЛЬНОЙ СЕТИ

Полноценное рассмотрение итогов развития интернета в контексте международной политики за последние годы можно сделать только в рамках целого ряда статей, в том числе составляющих настоящий выпуск журнала *Индекс Безопасности.* Выше обозначены лишь основные проблемы, которые обычно связывают с процессами *управления интернетом.* За пределами ее остались вопросы информационной безопасности, защиты сетевой инфраструктуры, контроля над распространением информации, прикладных аспектов интернет-технологий. Все эти вопросы также имеют собственную *политическую составляющую,* сравнимую с геополитикой сетевого адресного пространства, а зачастую и более ярко выраженную.

При этом подтверждается прежде высказанное предположение, что в последние годы основная тенденция заключается не столько в развитии интернета *вширь* (т. е. его распространения на новые страны, строительство новых линий связи и увеличения вычислительной мощности серверов), сколько *вглубь* — в создание новых ресурсов на национальных языках, появление новых функциональностей. Как ни парадоксально, но интернет становится все менее международным и более *домашним,* локализованным. Из достаточно экзотической игрушки *(окна в мир)* он превращается в *бытовое устройство* и необходимый инструмент ведения бизнеса. Видимо, именно в таких многообразных возможностях и заключается залог бесконечного совершенствования способов и методов применения Сети — ведь

приобретая новую функциональность, интернет-технологии не утрачивают свои прежние функции.

Подтверждается и вывод о том, что именно степень использования интернета в быту, в трудовой деятельности, в бизнес-процессах становится явным конкурентным преимуществом для стран, в которых для такого использования создаются наиболее благоприятные возможности, а значит, и государственные интересы таких стран все в большей степени должны учитываться при принятии решений, связанных с развитием Сети на глобальном уровне. В заинтересованном взаимодействии государства, бизнеса, общества лежит залог решения всех возникающих при использовании интернета проблем, в том числе связанных с расширением влияния интернет-технологий в международной политике.

Примечания

[1] Материал доработан на основе статьи: Якушев М. Управление интернетом: политика и геополитика. *Индекс Безопасности*. 2010, Лето. № 2 (93). С. 45–57.

[2] См., например: § 55. Как писать слово «интернет»? Студия Артемия Лебедева. 2000, 30 июня, http://www.artlebedev.ru/kovodstvo/sections/55/(последнее посещение — 30 августа 2012 г.).

[3] См., например: Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». *Российская Газета.* 2006, 29 июля, http://www.rg.ru/2006/07/29/informacia-dok.html (последнее посещение — 30 августа 2012 г.).

[4] Le Minitel, symbole d'une époque. Technologies. *Le Monde.fr.* 2012, June 29, http://www.lemonde.fr/technologies/portfolio/2012/06/29/le-minitel-symbole-d-une-epoque_1727096_651865.html (последнее посещение — 30 августа 2012 г.).

[5] См. Якушев М. Управление интернетом: политика и геополитика. *Индекс Безопасности*. 2010, Лето. № 2 (93). С. 45–57.

[6] Наиболее точный контекстный перевод англоязычного термина *stakeholders*.

[7] Подробнее см.: The Internet Governance Forum. Official Website, http://www.intgovforum.org (последнее посещение — 30 августа 2012 г.).

[8] См., например: Конвенция об обеспечении международной информационной безопасности (концепция). Национальная безопасность России. Совет Безопасности Российской Федерации, http://www.scrf.gov.ru/documents/6/112.html (последнее посещение — 30 августа 2012 г.).

[9] Assuring a Trusted and Resilient Information and Communications Infrastructure. Cyberspace Policy Review. The White House Official Website, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (последнее посещение — 30 августа 2012 г.).

[10] Brief History of the Internet. Internet Society, http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet (последнее посещение — 30 августа 2012 г.).

[11] Introduction to ISOC. Internet Society, http://www.isoc.org/isoc (последнее посещение — 30 августа 2012 г.).

Подробную информацию о структуре, организационных особенностях, функциях и развитии ISOC см. в статье в этом номере *Индекса Безопасности*: Касенова М. Глобальное управление интернетом в контексте современного международного права. С. 43–64.

[12] About the IETF. The Internet Engineering Task Force, http://www.ietf.org/about (последнее посещение — 30 августа 2012 г.).

[13] От англ. Request for Comments; иногда также переводится как запрос комментариев, однако все чаще используется в русских текстах в качестве аббревиатуры RFC без перевода. Подробнее см. статью в этом номере *Индекса Безопасности*: Касенова М. Глобальное управление интернетом в контексте современного международного права. С. 43–64.

[14] International Corporation for Assigned Names and Numbers, http://www.icann.org (последнее посещение — 30 августа 2012 г.).

[15] RIPE Network Coordination Centre, www.ripe.net (последнее посещение — 30 августа 2012 г.).

[16] Координационный центр национального домена сети Интернет, http:/www.cctld.ru (последнее посещение — 30 августа 2012 г.).

[17] Country Codes — ISO 3166. ISO 3166 Maintenance agency. ISO's focal point for country codes, International Organization for Standardization, http:/www.iso.org/iso/country_codes (последнее посещение — 30 августа 2012 г.).

[18] Applied-for New gTLD Strings. International Corporation for Assigned Names and Numbers. 2012, June 13, http://newgtlds-cloudfront.icann.org/sites/default/files/reveal/strings-1200utc-13jun12-en.pdf (последнее посещение — 30 августа 2012 г.).

[19] См., например:

Саудовская Аравия против новых доменных зон: .wtf, .vodka, .gay. *За рубежом*. 2012, 21 августа, http://www.gazetasng.ru/news/show/10082.html (последнее посещение — 30 августа 2012 г.).

Саудовская Аравия не одобрила домены.vodka и.gay. Координационный Центр национального домена сети Интернет. 2012, 16 августа, http://www.cctld.ru/ru/press_center/digest/detail.php?ID=3978 (последнее посещение 30 августа 2012 г.).

[20] International Corporation for Assigned Names and Numbers, http:/www.icann.org (последнее посещение — 30 августа 2012 г.).

Мадина Касенова

ГЛОБАЛЬНОЕ УПРАВЛЕНИЕ ИНТЕРНЕТОМ В КОНТЕКСТЕ СОВРЕМЕННОГО МЕЖДУНАРОДНОГО ПРАВА

История знает целый ряд открытий и изобретений, которые коренным образом изменили существование человека: бумага, письменность, порох, телеграф, радио, телевидение. К числу величайших изобретений конца 1960 гг., несомненно, относится и интернет. В настоящее время феноменальный успех интернета одновременно ввергает государства в своеобразную технологическую гонку вооружений и ведет к *интернетизации* значительного числа государств, расширяя и изменяя как географию, так и аудиторию интернет-пользователей.

В 1985 г. во всем мире насчитывалось приблизительно 20 тыс. *юзеров*, причем 90% из их числа составляли жители Соединенных Штатов. Спустя 20 лет, в 2005 г., численность пользователей интернета по всему миру приблизилась к 1,1 млрд человек, в том числе более 200 млн американцев, составлявших около 17% глобальной интернет-аудитории[1]. В 2011 г. около 44% всех интернет-пользователей мира приходилось на Азию, в Европе проживали порядка 23% пользователей, в США — 13%, а каждый десятый интернет-пользователь был жителем Латинской Америки[2]. Сегодня в мире насчитывается свыше четырех миллиардов цифровых телекоммуникационных устройств, к которым подключено более 1,6 млрд пользователей. В этих условиях с интернетом объективно связывается, с одной стороны, формирование и диверсификация многих социальных процессов. С другой стороны, особую актуальность приобретает собственно регулирование отношений в области интернета.

Вне всяких сомнений, сегодня интернет представляет собой центральный элемент инфраструктуры формирующегося информационного общества. Во многом по этой причине одним из ключевых в дискуссиях о глобальной сети всегда являлся и является вопрос о том, *кто* контролирует ее и управляет ей. В настоящее время этот вопрос не только не имеет однозначного решения — сами подходы к его разрешению весьма разнообразны. Существуют различные позиции относительно институтов и механизмов управления процессами и разработкой политики глобальной сети, создан целый ряд авторитетных научно-исследовательских учреждений, предметной сферой которых являются вопросы управления интернетом[3].

Попытка охватить систему и архитектуру управления глобальной сетью именно с международно-правового угла имеет исследовательскую ценность сразу по ряду причин.

Во-первых, трансграничный глобальный[4] характер интернета и ключевые особенности его функционирования, такие как саморегулирование, *сетецентричная* организация, отсутствие иерархии управления, — объективно сталкивают иссле-

дователя и управленца с целым комплексом проблем, задач и вопросов, решение которых осуществляется как на национальном, так и на международном уровнях. В силу специфики организации глобальной сети вопросы управления ей можно решать только совместными усилиями государств, международных межправительственных и неправительственных организаций, структур частного сектора и гражданского общества.

Во-вторых, проблематика управления интернетом рассматривается как самостоятельная предметная сфера и анализируется с позиций теории глобального управления, теории международных режимов, в политическом, социальном и прочих контекстах. При этом в рамках каждой теоретической модели термин *управление интернетом* (Internet Governance), понимается по-разному. Исходным в настоящей работе является определение, предложенное Рабочей группой по управлению интернетом (The Working Group on Internet Governance)[5].

В-третьих, интернет достаточно долгое время вообще не являлся предметом системного анализа специалистов в области международного публичного права, хотя в силу своей трансграничной природы он *должен был* стать таковым. Вопросы международно-правовой регламентации отношений в киберпространстве, применимости международного публичного права к интернету обрели практическую актуальность лишь в последнее десятилетие истории интернета, насчитывающей более 40 лет. Тем не менее в настоящее время анализ вопросов управления интернета плотно связан с международно-правовыми аспектами. В качестве базового подхода здесь выступает традиционное понимание международного права как системы договорных и обычных норм и принципов, выражающих согласованную волю государств и регулирующих отношения между ними, международными организациями и другими субъектами международного права.

В-четвертых, механизмы трансграничного — а по сути глобального — управления интернетом в системе современного международного права следует рассматривать как минимум на трех различных уровнях — институциональном, с обязательным учетом ключевой роли саморегулирования Сети. Однако именно институциональный механизм, на наш взгляд, является *системообразующим* для целей анализа.

ОБЩИЕ ПРИНЦИПЫ АРХИТЕКТУРЫ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Функционирование интернета предполагает, что глобальные информационные потоки и пакеты данных способны сами найти путь от отправителя к получателю. Существующая так называемая *физическая структура сети интернета* включает огромное количество преимущественно коммерческих сетевых операторов и собственно сетей — от небольших до межконтинентальных. Сетевые операторы могут, в зависимости от потребностей рынка, объединять и связывать свои инфраструктуры. В совокупности такие сети, формирующие *физическую структуру интернета*, оказываются связаны воедино в топологии, которая практически аналогична топологии развитой сети транспортных коммуникаций.

Неотъемлемой частью и одной из основ интернета является принцип саморегулирования. Тезис Брайана Карпентера о том, что интернет в определенном смысле представляет собой нейтральное пространство, которое существует без централизованного контроля[6], никому не принадлежит и никто не может его отключить, не теряет своей актуальности — однако фактически он не совсем корректен. *Центральный аппарат* управления и координации работы интернета существует, поскольку существует объективная необходимость выполнения, как минимум, трех конкретных функций.

Во-первых, речь идет о выработке принципов выделения блоков интернет-адреса пространства (IP-адрес). *Во-вторых*, имеется в виду эксплуатация корневых DNS-серверов, позволяющих подключенным к интернету устройствам находить друг

друга, а пакетам данных перемещаться от отправителей к получателям по всей сети интернет. Наконец, речь идет о выработке и внедрении принципов создания и администрирования национальных доменов верхнего уровня[7] и присвоения индексов имен интернет-доменов, например, таких как *.com*, .ru, *.info*, *.org*. и так далее.

Из сказанного становится ясно, что институциональный механизм глобального управления интернетом связан с деятельностью организаций, обеспечивающих его технологическое функционирование. Достаточно сложно, если вообще возможно, дать исчерпывающий перечень международных и национальных организаций, групп, форумов и иных структур, деятельность которых так или иначе связана с управлением интернетом. Также непросто, не избежав противоречий, определить их статус, компетенцию, порядок и систему взаимоотношений.

Основная причина столь сложной и дифференцированной глобальной архитектуры управления интернетом кроется в *дихотомии всемирной сети*. С одной стороны, она представляет собой техническое изобретение и, как таковое, объективно нуждается в технической поддержке и технологическом обеспечении своего функционирования. Если упростить понимание интернета до технического изобретения или технологического ресурса, решение вопроса об управлении им неизбежно перемещается в сферу деятельности структур, отвечающих за его поддержку и обеспечивающих его деятельность на техническом уровне. Поскольку функционирование глобальной сети невозможно без технического обеспечения, организации, выполняющие эти функции, имеют самое прямое отношение к системе управления интернетом и образуют *внутренний* институциональный механизм управления Сетью.

Вместе с тем глобальную сеть некорректно описывать лишь как техническое изобретение — она представляет собой феномен, оказывающий влияние на общемировое экономическое и социальное развитие. Интернет интегрирует материальные, финансовые, интеллектуальные, гуманитарные, политические, социальные и иные ресурсы, влияет на национальные и международные процессы социально-экономического плана и обеспечивает коммуникационные связи в планетарном масштабе. Всемирная сеть по своей технологической сути имеет международный, глобальный характер, в том числе и потому, что техническая и технологическая поддержка ее работы спроектирована именно под международный охват. Международный — в данном случае в значении *междустрановой* — характер интернета диктует саму логику его управления. Вопросы управления интернетом не могут рассматриваться и решаться вне глобального контекста. В этом смысле интернет предполагает существование внешнего, интернационализированного механизма управления.

Такой подход получил отражение в документах международных организаций и форумов. Например, резолюция Экономического и Социального Совета ООН (ЭКОСОС). Резолюция ЭКОСОС 2011/16 от 26 июля 2011 г.[8] разделяет вопросы, касающиеся интернета, на две большие группы, или *сферы*. С одной стороны, выделяется сфера интернета, относящаяся к «повседневной деятельности технического и эксплуатационного характера». С другой стороны, в документе рассматриваются сфера деятельности правительств и их роль в «выполнении своих обязательств в решении международных вопросов государственной политики, касающихся интернета». Данная сфера не связана с «деятельностью технического и эксплуатационного характера»[9] и рассматривается отдельно от нее.

И внутренний, и внешний институциональные механизмы управления интернетом взаимосвязаны, и однозначно выделить критерии их разграничения невозможно. Внутренний институциональный механизм управления интернетом к настоящему моменту в целом сформировался — поскольку сформировалась и устоялась внутренняя организационно-техническая модель функционирования интернета. Это, однако, не означает, что внутренний механизм в дальнейшем не будет развиваться и совершенствоваться.

Внешний, международный механизм управления интернетом находится в стадии формирования и становления. На его развитие, с одной стороны, влияет в целом сложившийся и действующий внутренний институциональный механизм управления интернетом. С другой стороны, в силу специфики трансграничного функционирования Сети во внешний институциональный механизм управления ей вовлечены государства, межправительственные организации, неправительственные организации, организации частного сектора, структуры гражданского общества. Столь разноуровневый состав участников системы управления интернетом дает основание ряду авторов связывать эту проблематику с «формированием новой модели многоуровневого глобального управления»,[10] «становлением новой архитектуры глобального управления»[11] и даже с «подрывом и размыванием вестфальской модели мира»[12].

На сегодняшний день центральными элементами *внешнего* механизма управления интернетом по-прежнему являются субъекты международного права, то есть государства и международные межправительственные организации.

ВНУТРЕННИЙ СТРУКТУРНО-ИНСТИТУЦИОНАЛЬНЫЙ МЕХАНИЗМ УПРАВЛЕНИЯ СЕТЬЮ

Анализ внутреннего институционального механизма управления интернетом следует начать с организаций, которые отвечают за технологическую поддержку глобальной сети и *централизованно* обеспечивают ее техническое функционирование. При таком подходе — и это принципиальный момент — *физическая инфраструктура сети* умышленно исключается из анализа, в силу того что вопросы, связанные с ее наличием и работой, по сути *вторичны.* Без соблюдения протоколов и параметров *физическая структура интернета* не может функционировать.

Подобный взгляд на вопросы управления глобальной сетью позволяет определить организации, которые обеспечивают технические аспекты ее функционирования, и выявить существующие между ними формальные и неформальные связи. Между этими организациями на сегодняшний день сложились постоянные устойчивые формальные и неформальные связи.

Организации, которые централизованно обеспечивают функционирование интернета на техническом уровне и осуществляют организационно-технический мониторинг Сети, можно условно распределить на несколько основных групп или центров, в рамках которых стоит особо выделить:

- Общество Интернета;
- Корпорацию Интернета по распределению имен и адресов;
- Консорциум Всемирной сети.

Общество Интернета [Internet Society, ISOC]

Развитие интернета, усложнение и диверсификация его инфраструктуры, расширение сфер его использования и нарастание потребности в формальной организации, которая взяла бы на себя функции центра, решающего вопросы стандартизации функционирования Сети, привели к образованию Общества Интернета. В 1991 г. был запущен процесс создания *ISOC* под эгидой Корпорации национальных исследовательских инициатив. Менее чем через год, в январе 1992 г. Общество Интернета было учреждено в форме некоммерческой корпорации, которая является юридическим лицом Федерального округа Колумбия, США.

Миссия *ISOC* заключается в содействии открытой разработке стандартов, протоколов, администрирования и технической инфраструктуры интернета, а также развитию национальной и международной политики с целью поддержки роста

и совершенствования сети интернет во всем мире[13]. *ISOC* обеспечивает не только организационную, но и юридическую базу для большинства организаций, отвечающих за разработку технических стандартов интернета. Общество Интернета оказывает содействие развитию национальной и международной политики с целью поддержки роста и совершенствования глобальной сети во всем мире. Практически все технологические стандарты интернета разрабатываются и устанавливаются группой организаций, входящих в *ISOC*.

В соответствии с Учредительным договором, в *ISOC* не создается уставного капитала, а организационная структура Общества построена по принципу членства, и ее деятельность финансируется в основном из членских взносов, пожертвований и спонсорских взносов. Членами Общества Интернета могут быть как физические, так и юридические лица, представители государств, международных организаций. Объем прав, которыми обладают члены *ISOC*, зависит от их статуса. По данным на середину 2012 г., Общество Интернета насчитывало более 55 тыс. индивидуальных членов по всему миру и более 130 организаций-членов в 180 странах мира. В частности, под эгидой *ISOC* действуют:

- Рабочая группа по проектированию интернета;
- Совет по архитектуре интернета;
- Рабочая группа по интернет-исследованиям;
- Руководящая группа по проектированию интернета;
- Руководящая группа по интернет-исследованиям;
- Редактор запросов на комментарии и предложения.

Перечисленные организации ответственны перед Обществом Интернета. Вместе с тем *ISOC* предоставляет им значительную степень независимости в их технической деятельности по развитию интернета и обеспечению доступности сети[14].

Основными правовыми документами *ISOC* является Договор об учреждении в редакции 1997 г. и Устав, действующий с изменениями и дополнениями от 2010 г. Поскольку *ISOC* является юридическим лицом Федерального округа Колумбия, США, ее деятельность подпадает под действие законодательства округа Колумбия и, в частности, Закона о некоммерческих организациях

За более чем 20-летнюю историю деятельности Общества Интернета его Учредительный договор фактически не претерпел изменений, в отличие от Устава. Последний периодически пересматривался с тем, чтобы обеспечить соответствие регламентов и процедур *ISOC* современным организационным стандартам, а также для того, чтобы деятельность *ISOC* соответствовала праву государства регистрации (в данном случае США). Последние изменения в Устав были внесены в июле 2011 г. Главным образом изменения и поправки Устава касались оптимизации институционального функционирования структуры *ISOC*, процедур выбора Попечителей, электронного голосования.

В соответствии с действующей редакцией Устава руководящим органом *ISOC* является Попечительский совет, который несет ответственность за деятельность *ISOC* в целом. В соответствии с положениями Устава, состав Попечительского совета включает не более 20 попечителей, если органом не будет принято иное решение по этому вопросу[15]. Попечители действуют в интересах интернет-сообщества в целом, но назначаются или избираются от следующих групп:

а) Отделений Общества Интернета

б) от организаций-членов *ISOC*;

в) от Группы по технологиям интернета.

В компетенцию Попечительского совета входит рассмотрение важнейших вопросов деятельности Общества и его структурных подразделений, включая внесение изменений в учредительные документы, вопросов распределения средств, решение финансовых вопросов и утверждение годовых отчетов, вопросы процедуры роспуска или ликвидации *ISOC*, утверждение регламентов и процедур и иных документов организации. Территориально Попечительский совет расположен в США, штат Вирджиния. Совет является консультативным органом высшего руководства *ISOC*, в чью которого входят вопросы, затрагивающие общую политику и эффективность функционирования интернета в глобальном масштабе.

Члены интернет-сообществ, разделяющие принципы и миссию *ISOC* и желающие участвовать в дальнейшем развитии технологии интернета в рамках того или иного географического района, могут быть объединены в Отделения *ISOC*. Процедура учреждения отделения регулируется процедурами учреждения и управления деятельностью отделения. Как правило, отделения действуют на основании уставов, которые разрабатываются и принимаются ими самостоятельно.

В рамках анализа целесообразно подробнее рассмотреть три структурных образования *ISOC*, взаимодействие которых в концентрированном виде отражает деятельность Общества и дает наглядное представление о внутреннем институциональном механизме управления интернетом.

Совет по архитектуре интернета [Internet Architecture Board, IAB]

Деятельность *IAB* связана с архитектурой глобальной сети, основу которой составляют Архитектурные принципы интернета, для которых также используется обозначение *RFC 1958*[16]. Данные принципы не только образуют основу технического проектирования интернета, но и отражают фундаментальные ценности интернет-сообщества в целом. К их числу относятся:

- ❑ принцип функциональной совместимости;
- ❑ принцип открытости;
- ❑ принцип сквозной связи;
- ❑ принцип отсутствия централизованного контроля.

В ряду архитектурных принципов интернета основным является принцип сквозной связи (*e2e*)[17], который зачастую оценивается как основополагающий архитектурный принцип глобальной сети, основа ее технологии и ориентир для органов управления при оценке ее изменений. Принцип *e2e* глубоко встроен в систему интернета и является основой для существующих интернет-протоколов.

В чисто техническом отношении *e2e* означает, что определенные обязательные сквозные функции могут выполняться надлежащим образом только конечными системами. В Архитектурных принципах интернета *RFC 1958* содержится следующая формулировка: «Задача сети заключается в наиболее эффективной и гибкой передаче дейтаграмм. Все остальное должно осуществляться конечными устройствами». На практике это означает, что в соответствии с принципом *e2e* интернет не выполняет никаких других функций, кроме эффективной передачи пакетов данных.

Принцип *e2e* в некотором смысле ограничивает функциональность интернета, поскольку он связан только с передачей пакетов данных от отправителя к получателю. Например, глобальная сеть сама по себе *не* осуществляет фильтрацию определенных пакетов данных в зависимости от их содержания, *не* проводит проверку прав доступа, *не* отслеживает прохождение пакетов данных, *не* вносит изме-

нения в данные, — интернет *только* обеспечивает отправку и доведение до адресата информационных пакетов[18].

Совет по архитектуре интернета курирует все вопросы, связанные с архитектурой интернета, включая его протоколы и другие стандарты[19]. Эту миссию IAB осуществляет по поручению Общества Интернета (*ISOC*) и, хотя в своей деятельности Совет обладает значительной степенью независимости, он все же подотчетен *ISOC*. Во-первых, IAB осуществляет консультирование Совета попечителей *ISOC* по вопросам, связанным с архитектурой интернета; во-вторых, Совет по архитектуре интернета выступает в качестве технического органа по внешним связям от имени *ISOC*.

В своей деятельности Совет по архитектуре интернета взаимодействует на формальной и неформальной основе со всеми структурами Общества Интернета. Так, IAB одновременно является комитетом IETF по техническим вопросам. Совет также является апелляционным органом по отношению к Руководящей группе по проектированию Интернета (Internet Engineering Steering Grup, IESG). При этом постановления Совета по архитектуре интернета, выносимые по решениям IESG, являются окончательными. Однако если есть основания полагать, что решение IAB было вынесено необоснованно, на него может быть подана апелляция в Совет попечителей *ISOC*.

Рабочая группа по проектированию интернета [Internet Engineering Task Force, IETF]

Рабочая группа была создана еще в 1986 г., она также не является юридическим лицом, занимается проектированием и архитектурой интернета и является основным органом, который разрабатывает, испытывает и внедряет новые технологические стандарты Сети, включая интернет-протоколы[20].

IETF представляет собой техническую группу, состоящую из сетевых администраторов, операторов, проектировщиков, исследователей, поставщиков, пользователей и так далее. Для осуществления своей технической работы та или иная группа разбивается на большие подразделения, называемые *направлениями*, каждым из которых руководит директор. Примечательно, что кандидатуры директоров направлений утверждаются Советом по архитектуре интернета (*IAB*). Направления подразделяются на более мелкие специализированные рабочие группы во главе с председателями[21].

IETF возглавляет председатель, кандидатура которого утверждается голосующими членами Совета по архитектуре интернета, *IAB*. Следует обратить внимание на организационную зависимость *IETF* от IESG: председатель *IETF* одновременно является председателем Руководящей группы по проектированию интернета. Кроме того, на решения председателей рабочих групп и руководителей направлений *IETF* распространяется право подачи апелляции в Руководящую группу. Наконец, на рассмотрение Руководящей группы вносятся разработанные *IETF* новые технологические стандарты интернета, включая протоколы.

IETF занимается проблемами технических аспектов организации интернета, а именно:

- осуществляет разработку спецификаций, стандартов и соглашений по общим архитектурным принципам протоколов Сети;
- принимает соответствующие рекомендации относительно стандартизации протоколов и выносит их на рассмотрение Руководящей группы по проектированию интернета;
- содействует широкому распространению технологий и стандартов, разрабатываемых в Исследовательской группе Интернет-технологий (IRTF).

Запрос комментариев [Request for Comments, RFC Editor]

RFC Editor представляет собой серию документов, в которых описывается набор интернет-протоколов и обобщается опыт функционирования Сети. Запросы комментариев содержат технические спецификации и рассматриваются как стандарты интернета, широко применяемые в глобальной сети. С 1969 по 1998 г. бессменным и единственным редактором *RFC* являлся Джон Постел[22]. Правами на *RFC Editor* обладает Общество Интернета. Ведение достоверного архива *RFC Editor*, управление данными документами, их редактирование и публикацию осуществляет по поручению *ISOC* Институт научной информации Университета Южной Калифорнии. Общую политику *RFC Editor* курирует и осуществляет *IAB*, а *ISOC* назначает лиц, работающих в *RFC Editor*, и финансирует его деятельность.

Упомянутые выше структуры — *IAB, IESG, IETF, IRSG, IRTF* и *RFC Editor* — по сути являются ассоциированными организациями, или подразделениями *ISOC*. Частично это объясняется тем, что *ISOC* координирует и финансирует множество мероприятий, связанных с развитием интернета. Кроме того, перечисленные организации тесно связаны между собой на организационном, структурном и функциональном уровнях. Авторитет *ISOC* весьма высок, однако, являясь юридическим лицом Федерального округа Колумбия, США, Общество Интернета не обладает статусом международной организации. По этой причине принимаемые им решения носят лишь рекомендательный характер.

Корпорация интернета по распределению имен и адресов [The Internet Corporation for Assigned Names and Numbers, ICANN]

Корпорация интернета по распределению имен и адресов (даже в России чаще называемая *ICANN*)[23] является организацией, осуществляющей контроль за системой присвоения доменных имен DNS (Domain Name System) и адресов в интернете и соблюдением базовых принципов данной системы. С самого начала своей истории *ICANN* имела особое значение в глобальной системе управления интернетом, так как вопрос управления Сетью был исходно поставлен и долгое время обсуждался исключительно в контексте борьбы за контроль над системой распределения доменных имен. В настоящее время этот контекст не только не теряет актуальности, но, напротив, приобретает новый импульс развития в связи с расширением зоны доменов верхнего уровня[24].

С момента создания *ICANN* в 1998 г. ее статус и функции определялись Учредительным договором, Уставом, а также Соглашением с Министерством торговли США, ранее курировавшим вопросы распределения имен и адресов в интернете. Соглашение между *ICANN* и Минторгом США получило название Меморандума о взаимопонимании[25]. Меморандум закреплял распределение доменных имен за *ICANN* и оставлял за федеральным правительством США осуществление надзорных функций за деятельностью Корпорации. В течение девяти лет взаимоотношения между ICANN и Министерством торговли США основывались на соответствующей версии Меморандума. За девять лет было заключено еще семь меморандумов. ICANN предоставило Министерству торговли США 13 отчетов о состоянии работ в соответствии с показателями и задачами, закрепленными в действующей версии Меморандумов о взаимопонимании.

Существовавшую систему взаимоотношений между правительством США и *ICANN* наглядно характеризует ряд примеров, в том числе дело о переназначении национального домена верхнего уровня *.iq* Ираком. Первоначально *ICANN* предоставила право на управление доменом *.iq* живущему в Техасе палестинцу Байану Элаши, однако вернула эти обязанности себе после того, как в 2002 г. Элаши был осужден за финансирование террористической организации. После американского вторжения в Ирак в 2003 г. Пол Бремер, глава временной администрации в Ираке, обратился к *ICANN* с просьбой выделить домен будущему

правительству Ирака, однако Корпорация отклонила заявку, мотивировав отказ тем, что Ирак еще не является достаточно стабильной страной. Только в ноябре 2005 г. иракские официальные лица смогли объявить о начале работы домена *.iq* в интернете[26].

Другой пример связан с известным делом по заявке на домен *.xxx.* В августе 2005 г. *ICANN* должна была вынести решение по заявке предпринимателя из Флориды относительно создания нового домена верхнего уровня *.xxx* для взрослых пользователей сети интернет. Принятие решения *ICANN* несколько раз откладывала по причине официального протеста со стороны правительства США. В частности, Министерство торговли США выразило озабоченность по поводу создания и регистрации домена верхнего уровня *.xxx* и направило председателю Совета директоров *ICANN* Винту Серфу соответствующее извещение. 10 мая 2006 г. Совет директоров *ICANN* проголосовал против заключения договора и отклонил заявку на регистрацию домена верхнего уровня *.xxx* [27].

На сегодняшний день эффективность работы *ICANN*, ее полномочия и деятельность, взаимодействие с существующими организациями в системе управлением интернетом подвергаются неоднозначной оценке со стороны международного интернет-сообщества. В частности, достаточно критично рассматривают статус и миссию *ICANN* американские исследователи. Например, Джонатан Вейнберг, анализируя проблему легитимности корпорации, отмечает отсутствие судебного надзора за принимаемыми ей решениями. По мнению исследователя, действующие процедуры принятия решений *ICANN* неадекватно отражают «неоднородность интернет-сообщества»[28].

Милтон Миллер высказывает мнение о том, что корпорация использует риторику по поводу сохранения саморегулирования интернета для «создания дымовой завесы вокруг реально проводимой ей политики и правовых аспектов управления интернетом»[29].

Михаэль Фрумкин в одной из работ, посвященных сравнительному анализу деятельности *ICANN* и *IETF*, приходит к выводу о том, что интернет-сообществу сложнее использовать площадку корпорации, чем площадку Рабочей группы по проектированию интернета. По утверждению эксперта, *ICANN* используется Министерством торговли США «в целях обхода Закона об административных процедурах и Конституции США, нарушая тем самым фундаментальные демократические ценности»[30].

Надо признать, что критика деятельности корпорации имеет под собой определенные основания. *ICANN* в значительной мере остается американской структурой, хотя бы потому, что является юридическим лицом штата Калифорния и подчиняется местным законам. И хотя в настоящее время корпорация формально не зависит от правительства США ни в политическом, ни в правовом отношении, нельзя говорить об отсутствии фактического влияния Белого Дома на ее решения. Рассмотрим этот момент несколько подробнее.

Специфический и не всегда принимаемый во внимание момент, касающийся нынешнего статуса *ICANN* и вопроса ее независимости от правительства США, состоит в том, что одна из ключевых структур, подконтрольных *ICANN* — Администрация адресного пространства интернет [Internet Assigned Numbers Authority, *IANA*] — по-прежнему связана соглашением с американским Министерством торговли. При этом непосредственно *IANA* осуществляет ряд ключевых для поддержания работы глобальной сети функций. Так, в ведении администрации находится управление пространствами IP-адресов, доменов верхнего уровня, а также регистрация параметров интернет-протоколов. Иначе говоря, *IANA* отвечает за распределение всех зарезервированных имен и номеров, которые используются в протоколах, определенных в *RFC Editor*.

В 2006 г. ICANN и Министерство торговли США заключили Соглашение о совместной деятельности (Joint Project Agreement, далее JPA), призванное содействовать

становлению ICANN как стабильной и независимой организации и уменьшить контроль со стороны Правительства США за деятельностью ICANN. В Соглашении закреплялись десять основных показателей, по которым Министерство торговли должно было оценивать эффективность работы ICANN и готовность корпорации к осуществлению своих функций в качестве независимой организации, учитывающей интересы всего международного интернет-сообщества. 30 сентября 2009 г., в последний день действия этого документа, было принято решение о том, что JPA продляться не будет. Вместо JPA было заключено соглашение под названием Подтверждение обязательств со стороны Министерства торговли США и Корпорации Интернета по распределению имен и адресов (Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation For Assigned and Numbers).

Однако прекращение действия JPA и заключение Affirmation of Commitments между ICANN и Министерством Торговли США не влияют на существующие обязательства по Соглашению, заключенному между Министерством торговли США и IANA. Соглашение продолжает действовать, несмотря на то, что IANA является структурным подразделением ICANN. Именно это обстоятельство дает основание ряду исследователей считать самостоятельность ICANN ограниченной.

Ситуация, при которой регламентация статуса и компетенции Администрации остались за пределами Устава ICANN, ведет к неоднозначной оценке ее правового положения. Так, целый ряд исследователей считают, что IANA следует рассматривать как дочернюю компанию ICANN, некоторые авторы полагают, что Администрация остается подконтрольной структурой правительства США. Последняя из этих двух точек зрения по большому счету подтверждается спецификой договорных отношений между Правительством США и ICANN. Поскольку IANA является ключевым звеном трансграничного управления интернета и ее функции в институциональном механизме Корпорации имеют принципиальное значение, вопрос о том, является ли IANA структурным подразделением ICANN, имеет далеко не праздный характер.

Суть международной дискуссии о необходимости реформирования системы управления интернетом сегодня во многом сводится к требованиям передачи под интернационализированный контроль (структур ООН) не столько полномочий *ICANN*, сколько функций *IANA*. Тем не менее без изменения статуса самой корпорации такой вопрос не решить — без функционала *IANA* вся повестка *ICANN* оказалась бы *полой*, а сама структура — практически не дееспособной. Сегодня вопрос остается на повестке дня, причем наиболее активно на международной арене его продвигает Россия, настаивающая на перераспределении полномочий корпорации и *де-факто* части функций *IANA* в пользу площадки Международного союза электросвязи. Главным событием 2012 г. в сфере управления интернетом должна стать Всемирная конференция по международной электросвязи МСЭ, которая состоится 3–14 декабря 2012 г. в Дубаи. Ожидается, что в рамках конференции РФ и ее союзники попытаются пролоббировать перераспределение ключевых полномочий ICANN — а скорее IANA — в пользу межправительственной глобальной площадки МСЭ.

Консорциум всемирной сети [World Wide Web Consortium, W3C]

W3C — независимая организация, деятельность которой сосредоточена на единых стандартах и протоколах интернета[31]. Членство в *W3C* открыто для любой организации и основывается на соглашении, заключаемом между ней и консорциумом. Учредители *W3C* — Массачусетский технологический институт в США, Европейский консорциум по исследованиям в области информатики и математики [*ERCIM*] в Европе и Университет Кейо в Японии. *W3C* — некоммерческая организация, то есть она не образует юридического лица. Руководящим органом Консорциума является Управляющий комитет, формирующий общую политику и стратегию для организации. Работа *W3C* строится по группам, распределяе-

мым в зависимости от стоящих перед ними задач. Возглавляет работу председатель, назначаемый Массачусетским технологическим институтом; в его компетенцию входят вопросы взаимодействия с членами *W3C* и развитие внешних связей консорциума.

Основная миссия *W3C* состоит в том, чтобы «полностью раскрыть потенциал Всемирной сети за счет разработки общих протоколов, которые способствуют ее эволюции и обеспечивают ее функциональную совместимость», а также испытания и внедрения новых технологических стандартов Сети[32]. В определенном смысле функции консорциума схожи с функциями *IETF*, которая осуществляет разработку технологических стандартов Сети. Однако деятельность консорциума более узконаправлена применительно к интернету и связанным с ним технологиям.

Членство в *W3C* определено таким образом, чтобы его участниками были организации, при этом не обязательно государственные или экспертные. Например, членами Консорциума являются такие компании, как *Adobe Systems Inc.*, *Boeing, Shevron, CityGroup* и целый ряд других компаний и организаций различных стран. Физические лица обладают ограниченными возможностями по участию в работе Консорциума; взаимодействие с ними строится в основном через публичные адресные списки *W3C*.

ВНЕШНИЙ СТРУКТУРНО-ИНСТИТУЦИОНАЛЬНЫЙ УРОВЕНЬ УПРАВЛЕНИЯ СЕТЬЮ

В силу особенностей интернета внешний институциональный механизм управления им формируется на многоуровневой основе. Элементами этого механизма являются государства, межправительственные организации, неправительственные организации, группы, структуры, коммерческие и некоммерческие организации, представляющие частный сектор и гражданское общество. В контексте институциональной структуры внешнего механизма управления интернетом указанные организации занимают неравнозначное положение.

Государства и международные организации есть субъекты международного права, и в этом смысле их роль в выполнении обязательств по решению международных вопросов государственной политики, касающихся интернета, первична. Неправительственные организации и структуры частного сектора и гражданского общества с точки зрения международного права являются вторичными субъектами глобального механизма управления интернетом. Однако их роль не следует преуменьшать, так как основой функционирования интернета является саморегулирование. Кроме того, нельзя забывать, что государства и международные организации включились в процесс институционализации управления Сетью лишь в последнее десятилетие, тогда как история интернета насчитывает более 40 лет.

Процесс институционализации внешнего механизма управления интернетом изначально осуществлялся в рамках межправительственных организаций. Кроме того, он был тесно связан с проведением Всемирной встречи на высшем уровне по вопросам информационного общества и последующих шагов по реализации принятых на встрече решений.

Всемирный саммит информационного общества[33] проходил под эгидой ООН. Встреча в полной мере отразила озабоченность мирового сообщества чрезмерной концентрацией основных рычагов управления глобальной сетью. Как отметили участники встречи, «очень узкий круг лиц обладает слишком большими полномочиями в части выработки политики развития глобальной инфраструктуры интернета»[34].

Саммит прошел в два этапа: в 2003 г. прошел первый, женевский этап, а в ноябре 2005 г. состоялся второй, тунисский. Важнейшим итогом первого этапа стало

появление первой в международной практике концепции управления интернетом. Другим важным результатом стало принятие двух документов, впоследствии одобренных Генеральной Ассамблеей ООН. Речь идет о Декларации принципов по вопросам информационного общества (далее Декларация принципов) и Плана действий Всемирной встречи на высшем уровне по вопросам информационного общества (далее План действий)[35].

Наконец, последним значимым итогом встречи стало учреждение Рабочей группы по управлению интернетом. В ходе второго этапа были приняты Тунисское обязательство по вопросам информационного общества и Тунисская программа для информационного общества[36]. Итоги тунисского этапа были закреплены специальной резолюцией Генассамблеи ООН[37].

Отмеченные выше особенности институционализации внешнего механизма управления интернетом дают основания считать, что международные межправительственные организации являются его центральными элементами. Формат данной статьи не позволяет осветить вопросы компетенции всех межправительственных организаций, как универсальных, так и региональных, включенных в процесс решения вопросов управления интернетом. Например, деятельность таких специализированных организаций ООН, как Международный союз электросвязи, Всемирная организация интеллектуальной собственности, ЮНЕСКО, составляет предмет специального исследования. Однако обозначить и кратко охарактеризовать основные межправительственные организации в этой сфере все же необходимо.

Понимание логики нынешнего развития глобальной архитектуры управления интернетом невозможно без анализа процессов, протекающих на площадках ООН. Система организаций ООН выступает в роли глобального форума по управлению интернетом, играет ключевую роль в содействии установлению связей и согласований усилий, направленных на развитие ИКТ в глобальном масштабе. Деятельность трех из шести главных органов ООН (Генассамблеи, ЭКОСОС и секретариата) напрямую связана с вопросами управления интернетом. Значительная роль в данной области также отводится Генеральному секретарю и Координационному совету руководителей ООН.

Группа ООН по информационному обществу [UN Group on the Information Society, UNGIS]

Особый интерес представляет новая структура организации — Группа ООН по информационному обществу. В соответствии с итоговыми документами Всемирного саммита, Генсеком ООН были проведены консультации с членами Координационного совета руководителей ООН по вопросу создания такой группы. *UNGIS* была создана по итогам консультаций в 2006 г. в качестве своеобразного *межучережденческого* механизма. Целью группы стала координация политики различных организаций в рамках структуры ООН в целях осуществления Женевского плана действий и Тунисской программы для информационного общества[38]. В этих целях UNGIS:

- способствует осуществлению *WSIS*, главным образом на международном уровне, путем включения в повестку дня *UNGIS* информации о мероприятиях и программ для членов *CEB*;
- координирует деятельность заинтересованных сторон в реализации решений тунисского этапа *WSIS* как на национальном, так и на региональном уровнях;
- содействует укреплению роли системы ООН в деле облегчения доступа развивающихся стран к новым и новейшим технологиям, поощрению передачи технологий, техники и инновационной политики, включая ИКТ;

- способствует взаимодействию между организациями системы ООН, чтобы максимально активизировать совместные усилия, избежать дублирования функций и повысить эффективность реализации решений *WSIS*;
- информирует общественность о том, как система ООН осуществляет решения *WSIS* и содействует улучшению доступа развивающихся стран к ИКТ.

Постоянными членами *UNGIS* являются Международный союз электросвязи (МСЭ), Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), Конференция Организации Объединенных Наций по торговле и развитию (ЮНКТАД), Экономическая комиссия Организации Объединенных Наций для Африки (ЭКАООН) и Программа развития Организации Объединенных Наций (ПРООН). Эти организации осуществляют функции председателя и заместителя председателя *UNGIS* на основе ротации. *UNGIS* имеет достаточно широкий членский состав непостоянных членов, в число которых входят специализированные организации ООН, и такие структуры, как Всемирная торговая организация (ВТО), Международное агентство по атомной энергии (МАГАТЭ), Международная организация труда (МОТ), Организация экономического сотрудничества и развития (ОЭСР) и прочие.

Рабочая группа по управлению интернетом [The Working Group of Internet Governance, WGIG]

Еще одна особенность внешнего институционального механизма управления интернетом связана с созданием и функционированием ряда различных структур, таких как всевозможные группы, комиссии, программы и форумы. Подобные структуры, во-первых, действуют на основании открытых мандатов межправительственных организаций. Во-вторых, они не имеют жесткой организационной структуры. В-третьих, они функционируют в качестве *открытой дискуссионной площадки* с привлечением заинтересованных участников. В-четвертых, их деятельность осуществляется на временной либо на постоянной основе. Наконец, принимаемые этими структурами решения, как правило, носят рекомендательный характер.

По итогам первого, женевского этапа *WSIS* Генеральный секретарь получил мандат ООН на учреждение Рабочей группы по управлению интернетом [The Working Group of Internet Governance, *WGIG*][39]. В рамках полученного мандата *WGIG* в течение 2003–2005 гг. провела четыре заседания. Основная деятельность *WGIG* была направлена на разработку рабочего определения понятия управления интернетом. Была проведена значительная работа по анализу существующих механизмов управления в государственном секторе, частном секторе и среди многочисленных заинтересованных сторон. При разработке рабочего определения понятия управления интернетом *WGIG* учитывала пять базовых критериев, а именно: рабочее определение должно быть адекватным, обобщенным, описательным, кратким и ориентированным на прикладные процессы.

По результатам анализа и дискуссий среди заинтересованных сторон, участвовавших в работе *WSIS*, было предложено определение, в рамках которого управление интернетом понималось как «*разработка и применение общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение интернета».* Субъектами данных действий в рамках определения выступила традиционная для концепции широкого участия всех заинтересованных сторон *триада,* состоящая из правительств, частного сектора и гражданского общества.

Рабочее определение управления интернетом исходит из признания того, что в конкретных вопросах управления интернетом каждая из перечисленных групп участников (или, используя распространенный англицизм, стейкхолдеров) имеет

собственные интересы, играет различные роли и принимает участие в различных форматах, которые зачастую дублируют друг друга. Вместе с тем поскольку управление интернетом не сводится к сетевым именам и адресам и тому подобным вопросам из повестки *ICANN*, участники Рабочей группы по управлению интернетом стремились к тому, чтобы рабочее определение понятия управления интернетом также включало другие важные вопросы государственной политики. В частности, определение должно было охватить проблематику важнейших интернет-ресурсов, вопросы безопасности интернета, перспективы развития и вопросы применения глобальной сети.

Еще одним направлением работы *WGIG* стало определение аспектов государственной политики, касающихся управления интернетом, и оценки адекватности существующих механизмов управления Сетью. В этой связи *WGIG* рассмотрела вопросы, связанные с государственной политикой, которые потенциально имеют отношение к управлению интернетом, определив четыре приоритетные области государственной политики:

- вопросы, имеющие непосредственное отношение к управлению интернетом и входящие в компетенцию отвечающих за них организаций. Сюда вошли вопросы, касающиеся инфраструктуры Сети и управления важнейшими интернет-ресурсами, включая административное управление системой имен доменов и адресами интернет-протокола (IP-адресами), управление системой корневых серверов, технические стандарты, корневое взаимодействие и соединение компьютеров, инфраструктуры телекоммуникаций, включая инновационные и конвергентные технологии, а также перевод сетей в многоязычный режим;
- вопросы, имеющие прямое отношение к управлению интернетом, но в большей степени связанные с практическим использованием интернета — спам, сетевая безопасность и киберпреступность;
- вопросы, связанные с интернетом, но имеющие далеко идущие последствия, выходящие за рамки интернета и лежащие в сфере ответственности соответствующих организации. К этой категории относятся, например, вопросы прав интеллектуальной собственности или международной торговли;
- вопросы, касающиеся прочих аспектов развития управлением интернетом; в частности, сюда относится задача расширения доступа к Сети в развивающихся странах.

WGIG также разработала рекомендации в отношении механизмов глобального управления интернетом, и предложила четыре организационные модели такого управления. Во всех из них упор был сделан на необходимости многостороннего сотрудничества в управлении Сетью и интернационализации институционального механизма такого сотрудничества. Кроме того, отмечалась необходимость координации деятельности различных организаций в системе управления интернетом на глобальном, региональном и национальном уровнях. Отметим, что все предложенные модели были связаны с деятельностью *ICANN*[40].

Важными аспектами деятельности *WGIG* были подготовка основы для проведения второго этапа Всемирной встречи и формулирование предложений относительно дальнейших мероприятий, связанных с управлением интернетом.

Форум по вопросам управления использованием интернета [The Internet Governance Forum, IGF]

Среди итогов второго, тунисского этапа *WSIS* интерес представляет Форум по вопросам управления использованием интернета [The Internet Governance Forum, *IGF*][41], созданный под эгидой ООН. Форум был учрежден для ведения

многостороннего политического диалога с участием всех заинтересованных сторон — правительств, частного сектора, коммерческих организаций, гражданского общества и межправительственных организаций[42]. Формат мандата Форума был определен пп. 72, 73 и 77 Тунисской программы и предусматривал пятилетний срок действия его деятельности.

В своей деятельности *IGF* опирается на существующий институциональный механизм управления использованием интернетом, уделяя при этом особое внимание взаимодополняемости функций всех структур, обеспечивающих функционирование интернета, и заинтересованных сторон, принимающих участие в этом процессе. Форум не выполняет надзорные функции, не подменяет существующие структуры, механизмы, институты или организации в сфере управления интернетом, не вмешивается в вопросы повседневной эксплуатации и технического обслуживания глобальной сети.

Открытый характер мандата не предусматривает жесткой организационной структуры Форума — она должна быть нейтральна, прозрачна, демократична и децентрализована, но ее конкретная конфигурация может периодически пересматриваться. Организационно *IGF* функционирует на постоянной основе через проведение ежегодных конференций, а также принимает участие в иных конференциях ООН по соответствующим вопросам.

Форум осуществляет свою деятельность в формате консультаций и рекомендаций, как это предусмотрено в различных статьях его мандата, и не принимает решений, имеющих обязательный характер. Поскольку мандат *IGF* включает в себя перечень приоритетных вопросов государственной политики, которые должны рассматриваться Форумом, его деятельность все же оказывает влияние на формирование и развитие внешнего институционального механизма управления интернетом. Перечень, который не является исчерпывающим, в частности, затрагивает следующие вопросы:

- обеспечение устойчивого характера, надежности, безопасности;
- стабильности и развития интернета;
- доступность и ценовая приемлемость интернета в развивающихся странах;
- возникающие проблемы;
- оценка практического осуществления принципов *WSIS* в процессе управления интернетом;
- вопросы, касающиеся важнейших ресурсов интернета;
- вопросы, возникающие в связи с надлежащим и ненадлежащим использованием интернета, имеющие особое значение для интернет-пользователей.

Вопросы государственной политики, рассмотренные в рамках форума, нашли отражение, например, в декларациях министров Совета Европы, и Организации экономического сотрудничества и развития (ОЭСР)[43].

За пятилетний период деятельности *IGF* произошла существенная динамика формата обсуждаемых вопросов, изменилось понимание их взаимосвязи. Например, если в 2006 г. вопросы открытости и безопасности обсуждались отдельно, то начиная с 2008 г. эти два вопроса, наряду с конфиденциальностью, стали рассматриваться вместе в контексте с такими вопросами, как доступ к знаниям, свобода выражения мнений, права интеллектуальной собственности, преступность в интернете и государственная безопасность. Явно смещаются акценты обсуждения проблемных сфер: в 2006 г. вопросы безопасности были увязаны с борьбой со спамом, а в 2010 г. тема безопасности была расширена за счет включения в нее вопроса о регулировании вредоносного контента[44].

С 2011 г. обсуждается вопрос о том, чтобы сделать бюджет форума в рамках ООН более регулярным и превратить *IGF* в официальный орган межправительственного механизма ООН в качестве меры по укреплению связи с выработкой государственной политики. Цель подобных мер их авторы видят в том, чтобы «дать государствам-членам право требовать от *IGF* конкретные доклады в формате, пригодном для обсуждения на межправительственном уровне»[45].

Необходимость продолжения функционирования форума была подтверждена соответствующими рекомендациями Генерального секретаря ООН и резолюциями Генеральной Ассамблеи ООН. В 2010 г. было принято решение продлить мандат Форума еще на пять лет, проанализировать его деятельность в контексте 10-летнего периода выполнений решений *WSIS* в 2015 г., а также рассмотреть вопросы совершенствования формата, функций и деятельности *IGF*[46].

ВЫНУЖДЕННОЕ СОТРУДНИЧЕСТВО?

Интернет в настоящее время рассматривается в качестве одного из важнейших элементов жизненно важной, критической инфраструктуры государства и нуждается в не менее надежной системе безопасности, чем любая подобная инфраструктура[47]. Технические компоненты глобальной сети подпадают под многочисленные национальные и государственные юрисдикции, которые могут регулировать интернет и накладывать ограничения на сетевой контент. Однако ни одно государство не обладает монопольной властью над интернетом уже в силу его децентрализованности и саморегулируемой природы. Глобальная сеть в смысле регулирования стала своеобразным *капканом* для государств, по мере того как назрели вопросы, связанные с необходимостью развития и совершенствования механизмов управления ей.

В этих условиях очевидно, что государства, с одной стороны, находятся в ситуации своеобразной технологической гонки вооружений, которую провоцирует бурное развитие интернет-технологий. С другой стороны, поскольку функционирование интернета имеет трансграничный, глобальный характер, вопросы управления Сетью должны решаться в соответствующем масштабе. Это обстоятельство вынуждает государства к сотрудничеству, что *предполагает совместное использование международно-правовых институтов и механизмов.*

Однако сотрудничество в этой области отнюдь не ограничивается межправительственным форматом. Круг участников процесса глобального управления интернетом слишком широк для того, чтобы государства в одиночку могли адекватно транслировать, учитывать и согласовывать их интересы. Национальные правительства взаимодействуют с международными межправительственными и неправительственными организациями, представителями частного сектора, гражданского и экспертного сообщества. Подобное взаимодействие осуществляется в рамках форумов, рабочих групп и прочих форматов и требует активного привлечения инструментария международного права.

Эффективность участия государства в решении вопросов глобального управления интернетом зависит не только от того, как само государство действует на межгосударственном уровне и в рамках международных организаций, не менее значимым параметром является то, насколько активно *представители* этого государства — эксперты, специалисты частного сектора, структуры гражданского общества — действуют в рамках многочисленных международных площадок и форматов, деятельность которых сосредоточена на вопросах управления глобальной сетью. Этот тезис особо актуален, если коснуться вопроса о продвижении российских национальных интересов в сфере глобального управления интернетом.

В этой связи показательны два лаконичных примера.

Первый. Данные совместной резолюции Генеральной Ассамблеи ООН и Экономического и Социального Совета ООН, представленные в *табл. 1,* отражают некоторые показатели работы *IGF*[48]. В четвертом совещании форума, которое прошло в Шарм-эш-Шейхе, Египет, в ноябре 2009 г., приняли участие многочисленные заинтересованные группы из всех регионов мира и более чем 80 государств и территорий.

Таблица 1. **Количественные показатели состава участников четвертого совещания Форума по вопросам управления интернетом (IGF), 2009 г.**

Заинтересованная группа	Число стран или территорий	Число делегаций	Число участников
Правительства			
Развитые страны	32	46	136
Африка	21	53	272
Азия и Тихий океан	22	41	88
СНГ	3	5	7
Латинская Америка и Карибский бассейн	6	11	26
Итого	84	156	529
Частный сектор			
Развитые регионы	17	70	119
Африка	5	29	49
Азия и Тихий океан	8	14	15
СНГ	0	0	0
Латинская Америка и Карибский бассейн	2	2	3
Итого	32	115	188
Гражданское общество			
Развитые регионы	23	171	317
Африка	21	53	272
Азия и Тихий океан	18	42	76
СНГ	3	5	9
Латинская Америка и Карибский бассейн	11	15	26
Итого	71	283	544

Второй. В январе 2012 г. в Женеве, Швейцария, прошло очередное заседание Рабочей группы по управлению использованием Интернет (*WGIG*). РФ на мероприятии представляла исключительно правительственная делегация, в то время как российский частный сектор и структуры гражданского общества полностью проигнорировали заседание.

Практический смысл этих (и многих им подобных) примеров применительно к Российской Федерации сводится к удручающей пассивности выразителей нацио-

нальных интересов нашей страны в вопросах управления интернетом на международной арене. Как видно из статистических данных первого примера, Россия (которая в основном и представляет СНГ на подобных форумах), существенно отстает по показателям участия даже от таких регионов, как Карибский бассейн и Африка. При этом упрек в пассивности следует, как ни странно, адресовать прежде всего не государству, а частному сектору и гражданскому обществу, которые весьма скупо представлены на мероприятиях подобного рода.

Возможно, статистика участия в ключевых дискуссиях по управлению глобальной сетью и не отражает расстановки сил в кулуарах международной дипломатии. И в то же время, может ли страна, чей голос на официальных дискуссионных площадках составляет менее двух процентов от общего *хора*, успешно продвигать такие серьезные инициативы в системе управления Сетью, как изъятие части ключевых полномочий у *ICANN*? И могут ли представители бизнеса и экспертного сообщества предъявлять властям претензии по поводу невнятного курса в области управления интернетом, если сами отказываются от участия в диалоге по этим вопросам? При этом речь идет не формально-протокольных дискуссиях, а о процессе многосторонней выработки решений в области глобальной политики. Развивая эту логику, следует задать еще один вопрос: нет ли противоречия в том, что российские эксперты, бизнесмены, *интернетчики* и гражданские активисты, справедливо критикуя власти за слабый учет их мнения и принципов мультистейкхолдеризма в сфере национального регулирования Сети, не исполняют собственные обязанности стейкхолдеров на международной арене?

Конечно, такие вопросы выходят далеко за рамки международно-правовой проблематики управления интернетом, которой посвящена эта статья. Однако необходимо помнить, что международное право не является *вещью-в-себе* и не существует ради самого себя. В конечном счете оно являет собой механизм согласования национальных интересов и обеспечения их справедливого баланса на глобальном уровне. И для того чтобы перспективная архитектура и система управления Сетью максимально отвечала потребностям и запросам граждан России, этот механизм должен интенсивно и эффективно ими использоваться, в том числе в части площадок для согласования подходов и дискуссии, которые он предоставляет.

Примечания

[1] См. подробнее: Internet User Forecast by Country. An Estimate and Forecast of Internet Users in 57 Countries and 6 Regions of the World. ETForecasts. http://www.etforecasts.com/products/ES_intusersv2.htm (последнее посещение — 30 августа 2012 г.). Также см.: Internet World Stats. Usage and population statistics. http://www.internetworldstats.org (последнее посещение — 30 августа 2012 г.).

[2] Число пользователей интернета в мире превысило 2 млрд. *Проект РИА Новости Digit*. 2012. 19 января. http://www.digit.ru/internet/20120119/388740596.html (последнее посещение — 30 августа 2012 г.).

[3] См. подрбнее: Oxford Internet Institute. University of Oxford. http://www.oii.ox.ac.uk (последнее посещение — 30 августа 2012 г.); The Center for Internet and Society at Stanford Law School. http://cyberlaw.stanford.edu (последнее посещение — 30 августа 2012 г.); Berkman Center for Internet&Society at Harvard University. http://cyber.law.harvard.edu (последнее посещение — 30 августа 2012 г.); Internet Governance Project. Syracuse University http://www.igp.org (последнее посещение — 30 августа 2012 г.).

[4] Понятия *глобальный* и *трансграничный* рассматриваются в настоящей статье как тождественные.

[5] См.: Report of the Working Group on Internet Governance. Château de Bossey. June 2005. http://www.wgig.org/docs/WGIGREPORT.pdf (последнее посещение — 30 августа 2012 г.). Отметим, что в документах международных организаций термины *управление использованием интернета* и *управление интернетом* употребляются как тождественные.

[6] *Carpenter B.* The Architectural Principles of the Internet. Network Working Group. June 1996. http://www.dbj.rt.bw.schu.de/feacher/info/rfc/rfc.htm (последнее посещение — 30 августа 2012 г.).

[7] Procedures and Guides. Country-code Top-level Domain specific-information. Internet Assigned Numbers Authority. http://www.iana.org/cctld/cctld.htm (последнее посещение — 30 августа 2012 г.).

[8] Оценка прогресса, достигнутого в осуществлении решений и последующей деятельности по итогам Всемирной встречи на высшем уровне по вопросам информационного общества (E/2011/31). Основная сессия 2011/16. 2011. 16 июля. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan047549.pdf (последнее посещение — 30 августа 2012 г.).

[9] Резолюции и решения, принятые Экономическим и Социальным Советом на его организационной, возобновленной организационной и основной сессиях 2011 года. E/2011/INF/2. Экономический и Социальный Совет. 2011. 22 августа. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan047362.pdf (последнее посещение — 30 августа 2012 г.).

[10] Kleinwächter W. Internet Co-Governance. Towards a Multilayer Multiplayer Mechanism of Consultation, Coordination and Cooperation (M3C3) E–Learning. 2006. No. 3 (3). http://www.wwwords.co.uk/pdf/viewpdf.asp?j=elea&vol=3&issue=3&year=2006&article=18_Kleinwachter_ELEA_3_3_web&id=212.16.10.52 (последнее посещение — 30 августа 2012 г.). Также см.: Raboy M. The World Summit on the Information Society and its legacy for global governance. *The International Journal for Communication Studies*. 2004. № 3–4 (66). С. 225–232.

[11] См. Mathiason J. Internet Governance: The New Frontier of Global Institutions. London: Taylor & Francis, 2008. С. 32; Малаян Р. Международные организации в формирующемся миропорядке. Космополис. 2008. № 1 (20). http://cosmopolis.mgimo.ru/index.php?option=com_content&task=view&id=171 (последнее посещение — 30 августа 2012 г.).

[12] См., например: Барабанов О. История мировой политики. М.: МГИМО. 2006. С. 56–58.

[13] В создании ISOC принимали участие Винт Серф (Vinton G. Cerf) и Роберт Кан (Robert E. Kahn), являющиеся одними из отцов-основателей Интернета. См. подробнее: Mission. Internet Society. http://www.isoc.org/isoc/mission/(последнее посещение — 30 августа 2012 г.). Vinton Cerf — TCP/IP Co-Designer. The Internet. The Wordl's First Web Published Book (2000). http://www.livinginternet.com/i/ii_cerf.htm (последнее посещение — 30 августа 2012 г.).

[14] См. подробнее: Internet Society. http://www.isoc.org (последнее посещение — 30 августа 2012 г.). Также о структуре ISOC см., например: Кубалийя Й. Управление Интернетом. Й. Курбалийя. Координационный центр национального домена сети Интернет. М., 2010. С. 172–174.

[15] За исключением первоначального Попечительского совета, поименный состав которого был указан в Учредительном договоре организации.

[16] Request for Comments (RFC), то есть фундаментальные интернет-протоколы, их сочетание, возможность разработки новых. RFC 1958 назван Архитектурные принципы Интернета. См. подробнее: *Carpenter B.* Architectural Principles of the Internet. Internet Engineering Task Force. The Internet Society. http://www.ietf.org/rfc/rfc1958.txt (последнее посещение — 30 августа 2012 г.).

[17] Принцип сквозной связи впервые выдвинули Джером Сальцер, Дэвид Рид и Дэвид Кларк (Jerome Saltzer, David Reed, David Clark). См. подробнее: Saltzer J., Reed D., Clark D. End-to-End Arguments in System Design. M. I. T. Laboratory for Computer Science. http://www.reed.com/Papers/EndtoEnd.html (последнее посещение — 30 августа 2012 г.).

[18] Такую оценку принципа e2e разделяют не все исследователи: По мнению Джонатана Зиттрана (Jonathan Zittrain), например, узкая сфокусированность на принципе сквозной связи игнорирует возможности сложного взаимодействия между компьютером и интернетом как

генерирующей системы. См. подробнее: Zittrain J. The Generative Internet http://www.oiprc.ox.ac.uk/papers/EJWP0306.pdf (последнее посещение — 30 августа 2012 г.).

[19] Interne Architecture Board. http://www.iab.org (последнее посещение — 30 августа 2012 г.).

[20] Робачевский А. Где рождаются стандарты Интернета. Российский НИИ развития общественных сетей (РосНИИРОС). http://www.ripn.net/articles/ietf-intro/(последнее посещение — 30 августа 2012 г.).

[21] Деятельность IETF и комитетов носит открытый характер и обсуждается на соответствующих сайтах. См. подробнее: Internet Research Task Force (IRTF). http://www.irtf.org/(последнее посещение — 30 августа 2012 г.). The IESG. The Internet Engineering Task Force Website. http://www.iesg.org/(последнее посещение — 30 августа 2012 г.). IETF Administrative Support Activity (IASA). http://iaoc.ietf.org/(последнее посещение — 30 августа 2012 г.).

[22] Джон Постел (Jonathan Postel) — один из *отцов-основателей* интернета, участвовал в создании около 200 RFC и фактически именно он превратил RFC в стандарт интернета.

[23] История, структура, принципы функционирования, логика реформирования ICANN и ее место в современной системе глобального управления интернетом рассматриваются на страницах настоящего номера *Индекса Безопасности*. См.: Якушев М. Интернет–2012 и международная политика. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 38–40.

[24] Подробно о расширении доменного пространства также см. статью в этом номере *Индекса Безопасности*: Якушев М. Интернет–2012 и международная политика.

[25] См. подробнее: Memorandum of Understanding Between the U. S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers. ICANN. 1999. 31 December. http://www.icann.org/general/icann-mou-25nov98.htm (последнее посещение — 30 августа 2012 г.).

См. также: Бабкин С. Интеллектуальная собственность в Сети Интернет. М.: Юристъ, 2006. С. 212–213

[26] Bul B. The.iq Debacle. Foreign Policy. 2005. August 30. http://www.foreignpolicy.com/story/cms.php?story_id=3207 (последнее посещение — 30 августа 2012 г.).

[27] Следует отметить, что ситуация с регистрацией домена.xxx развивалась довольно стремительно. 20 июня 2010 г., после «получения независимости», ICANN зарегистрировал этот домен. См. подробнее: Mayer-Schönberger V., Ziewitz M. Jefferson Rebuffed: The United States and the Future of Internet Governance. The Columbia Science and Technology Law Review. 8 Colum. 188 (2007). http://www.stlr.org/html/volume8/schoenbergerintro.php (последнее посещение — 30 августа 2012 г.). См. также о создании домена.*xxx*: Feds Urge Delay for. XXX Domain. *Wired.* 2005. August 16. http://www.wired.com/techbiz/it/news/2005/08/68545 (последнее посещение — 30 августа 2012 г.).

[28] Weinberg J. Non-State Actors and Global Informal Governance — The Case of ICANN. Social Science Research Network. 2010. June 7. http://faculty.law.wayne.edu/Weinberg (последнее посещение — 30 августа 2012 г.).

[29] Mueller M. ICANN and Internet Governance. Sorting Through the Debris of 'Self-Regulation'. *Camford*. Vol.1 No.6. December 1999. http://www.icannwatch.org/archive/mueller_icann_and_internet_governance.pdf (последнее посещение — 30 августа 2012 г.). Mueller M., Mathiason J., Klein H. The Internet and Global Governance: Principles and Norms for a New Regime. Global Governance. 2007. No 13. http://139.179.20.111/Governance/ggov.2007.13.2.pdf (последнее посещение — 30 августа 2012 г.).

[30] Froomkin M. Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution. University of Miami Website. http://personal.law.miami.edu/~froomkin/articles/icann-main.htm (последнее посещение — 30 августа 2012 г.).

[31] W3C был основан Тимом Бернерсом-Ли (Sir Timothy John Berners-Lee) в 1994 г. в Массачусетском технологическом институте совместно с Европейской организацией ядерных исследований (CERN).

[32] World Wide Web Consortium (W3C) Official Webste. http://www.w3.org/(последнее посещение — 30 августа 2012 г.).

[33] См. подробнее: Резолюция Генеральной Ассамблеи 58/201. Политическое послание Комитета Министров на Всемирной встрече на высшем уровне по вопросам информационного общества (WSIS) (Женева 10–12 декабря 2003 г.). Генеральная Ассамблея. Организация Объединенных Наций. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/450/77/PDF/N0345077.pdf?OpenElement (последнее посещение — 30 августа 2012 г.).

[34] Basic Information: Abut WSIS. World Summit on the Information Society. Geneva 2003 — Tunis 2005. http://www.itu.int/wsis/basic/about.html (последнее посещение — 30 августа 2012 г.).

[35] A/RES/59/220. Всемирная встреча на высшем уровне по вопросам информационного общества. Резолюция, принятая Генеральной Ассамблеей [по докладу Второго комитета (A/59/480)]. Генеральная Ассамблея. Организация Объединенных Наций. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/489/48/PDF/N0448948.pdf?OpenElement (последнее посещение — 30 августа 2012 г.). См. также: First Phase of the WSIS (10–12 December 2003, Geneva). Geneva Plan of Action. WSIS-03/GENEVA/DOC/0005. World Summit on the Information Society. http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!! PDF-E.pdf (последнее посещение — 30 августа 2012 г.). First Phase of the WSIS (10–12 December 2003, Geneva). Geneva Declaration of Principles. WSIS-03/GENEVA/DOC/0004. World Summit on the Information Society. http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!! PDF-E.pdf (последнее посещение — 30 августа 2012 г.).

[36] Second Phase of the WSIS (16–18 November 2005, Tunis). Tunis Commitment. WSIS-05/TUNIS/DOC/7. World Summit on the Information Society. http://www.itu.int/wsis/docs2/tunis/off/7.pdf (последнее посещение — 30 августа 2012 г.). Second Phase of the WSIS (16–18 November 2005, Tunis). Tunis Agenda for the Information Society. WSIS-05/TUNIS/DOC/6 (rev. 1). World Summit on the Information Society. http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf (последнее посещение — 30 августа 2012 г.).

[37] WSIS Outcome Documents. World Summit on the Information Society. http://www.itu.int/wsis/index.html (последнее посещение — 30 августа 2012 г.).

[38] Outcome Document. WSIS Forum 2011. 16–20 May Geneva. http://groups.itu.int/wsis-forum2011 (последнее посещение — 30 августа 2012 г.).

[39] Председателем WGIG являлся и является в настоящее время Нитин Десаи (Nitin Desai), специальный советник Генерального секретаря ООН по WSIS.

[40] Background Report. The Working Group on Internet Governance. June 2005. World Summit on the Information Society. http://www.itu.int/wsis/wgig/docs/wgig-background-report.pdf (последнее посещение — 30 августа 2012 г.).

[41] The Internet Governance Forum. http://www.intgovforum.org (последнее посещение — 30 августа 2012 г.).

[42] WSIS Implementation, Follow-Up and Review Process. World Summit on the Information Society. http://www.itu.int/wsis (последнее посещение — 30 августа 2012 г.).

[43] Совет Европы выступает в защиту принципа нейтралитета в интернете. *Вестник Европы The Herald of Europe.* 2011. № 30. http://magazines.russ.ru/vestnik/2011/30/ne13.html (последнее посещение — 30 августа 2012 г.).

[44] Continuation of the Internet Governance Forum. Note by the Secretary-General. Economic and Social Council. Substantive session of 2010. New York, 28 June-23 July 2010. A/65/78.E/2010/68. General Assembly. Economic and Social Council. The United Nations. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan039400.pdf (последнее посещение — 30 августа 2012 г.).

[45] Там же.

[46] Information and communications technologies for Development. Resolution adopted by the General Assembly [on the report of the Second Committee (A/65/433)]. A/RES/65/141. General Assembly. The

United Nations. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/521/00/PDF/N1052100.pdf?OpenElement (последнее посещение — 30 августа 2012 г.).

[47] См., например: International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. The White House Official Website. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (последнее посещение — 30 августа 2012 г.). The UK Cyber Security Strategy/. Protecting and promoting the UK in a digital world. November 2011. Cabinet Office. http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy (последнее посещение — 30 августа 2012 г.).

[48] См. подробнее: A/65/68-E/2010/68. Продолжение деятельности Форума по вопросам управления Интернетом. Записка Генерального секретаря Организации Объединенных Наций. Генеральная Ассамблея. Экономический и социальный совет. 2010. 7 мая. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan039403.pdf (последнее посещение — 30 августа 2012 г.).

Олег Демидов

СОЦИАЛЬНЫЕ СЕТЕВЫЕ СЕРВИСЫ В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ И НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ[1]

Весной 2011 г. страны Магриба и Ближнего Востока захлестнула небывалая волна социальных протестов, повлекшая за собой отставку режимов в одних странах, репрессии вперемежку с лихорадочными реформами в других, а кое-где — гражданскую войну и фактический крах государственности. Эти события, отозвавшиеся эхом на огромном пространстве от Судана до Белоруссии, стали известны как *Арабская весна* и *твиттер/фейсбук-революции*. Второе из упомянутых названий отражает черту, характерную для большинства эпизодов ближневосточных протестов, — беспрецедентно активное использование участниками протестов информационно-коммуникационных технологий (ИКТ), и в первую очередь социальных сетевых сервисов. После волнений 2009 г. в Иране и Молдавии в рядах политиков, экспертов и СМИ прочно закрепился дискурс «ИКТ (и прежде всего соцсети) как главный двигатель волнений и революций *Арабской весны*».

Безобидная технология, призванная упростить досужее общение, приобрела черты оружия массового уничтожения (ОМУ), угрожающего стабильности и безопасности отдельных стран и международного сообщества в целом. Споры о роли социальных сетей в *Арабской весне* сегодня определяют основную суть дискуссии вокруг них, однако круг связанных с ними вопросов в рамках проблематики безопасности, конечно, гораздо шире.

Задача этой статьи состоит в том, чтобы проанализировать социальные сетевые сервисы и их влияние на развитие современного мира с позиций безопасности. Ключевой вопрос состоит в том, каким образом следует, с учетом тенденций последних лет, а также недавних и продолжающихся *революций онлайн* на Ближнем Востоке и в других регионах, рассматривать влияние социальных сетевых сервисов на международную безопасность, а также на национальную безопасность РФ. Этот вопрос влечет за собой еще два вопроса, первый из них — стоит ли рассматривать социальные сетевые сервисы как вызов, угрозу, либо, напротив, потенциальный фактор укрепления безопасности и технологию, способствующую ее обеспечению? Второй вопрос, рассматриваемый прежде всего на примере России, касается того, каков должен быть государственный политический курс, призванный учитывать развитие сетевых интернет-технологий и использовать его для укрепления безопасности.

Наконец, отдельным вопросам в рамках анализа является рассмотрение курса США в области использования ИКТ, и в том числе социальных сетевых сервисов для решения задач внешней политики. В частности, предпринимается попытка определить, несет ли подход Соединенных Штатов вызовы для международной безопасности, и если да, то в какой мере они обусловлены акцентом на использование социальных сетей и подобных им технологий.

Анализ упомянутой проблематики ведется с политологической точки зрения, не претендуя на правовую и техническую экспертизу. Рассмотрение социальных сетей в контексте безопасности, вынесенное в заголовок статьи, предполагает уход от правовых акцентов, рассмотрение и употребление таких понятий, как «национальная безопасность», «международная безопасность», вне специфического правового контекста. Технические аспекты проблематики смещены на задний план либо опущены в силу того, что не являются основным объектом анализа и требуют отдельных исследований. Они рассматриваются лишь в той мере, в которой необходимы для понимания изучаемой проблематики.

СОЦИАЛЬНЫЕ СЕТЕВЫЕ СЕРВИСЫ — ГРАНИЦЫ ПОНЯТИЯ

Объектом анализа в статье выступают социальные сетевые сервисы, хотя такая формулировка не является единственно приемлемой для рассматриваемого явления. Употребляются и такие термины, как «социальные сети», «социальные сетевые сообщества» и «социальные медиа». Во всех случаях речь идет о совокупности виртуальных сервисов и платформ, функцией которых является создание горизонтальных (т.е. сетевых) социальных связей между их пользователями. Русскоязычные обозначения являются кальками англоязычных терминов (social networking services, social network sites), более точно отражающих суть данного явления. В техническом смысле социальные сетевые сервисы являют собой классический пример Web 2.0. Так зачастую называют принцип проектирования систем, которые улучшаются и совершенствуются за счет возможностей сетевого взаимодействия и участия в нем широкого, не ограниченного изначально круга пользователей.

Единственное необходимое уточнение касается внутренней классификации социальных сервисов и ее оснований. В рамках статьи выделяются две категории таких сервисов:

а) собственно социальные сети — как универсальные, так и специализированные, профессиональные (*Facebook*, *Одноклассники*, *ВКонтакте*, *LinkedIn*, *MySpace*, *Friendster*, *Google+* и пр.);

б) квазисоциальные сообщества (блоговые сообщества, микроблоговые сервисы (*Twitter*), сообщества на интерактивных платформах типа *Ushahidi* и т. д. — данный перечень является открытым).

Провести четкое разграничение между обозначенными категориями достаточно сложно. Те же блоги могут быть лишь отдельным сервисом в рамках социальных комьюнити, обычные сайты могут иметь развитые социальные закладки, геосоциальные сети могут работать просто как сервис определения местонахождения, а могут приобретать полноценные социальные функции.

Можно лишь выделить тот перечень характеристик, которые в совокупности позволяют назвать тот или иной сервис социальной сетью. Подобный перечень был сформирован в еще в 2008 г. в примечательном исследовании *Social Network Sites: Definition, History, and Scholarship*. Его авторы выделили три ключевые характеристики *сайта социальной сети* (social network site)[2]. Речь идет о возможности создания личного профиля пользователя, хотя бы частично открытого для других людей, управлении списком пользователей, с которыми поддерживается связь, и возможности просмотра и отслеживания связей других пользователей.

Приведенный перечень, вероятно, нуждается в единственном уточнении: характеристики профиля пользователя должны иметь значение для социальной коммуникации. Геолокационный сервис не будет геосоциальной сетью, если к возможности определения координат пользователей не добавить их социально значимые характеристики — пол, возраст, хобби, цель посещения тех или иных локаций и т. д. Соответственно, все те сетевые сервисы, в которых отсутствуют какие-либо из перечисленных возможностей, относятся к *квазисоциальным сетям*.

Подобная классификация носит общий характер и не отражает многочисленных технологических нюансов, однако она допустима для целей этого исследования. Более подробная классификация социальных сетевых сервисов представлена в исследовании IEEE Computer Society за 2008 г.[3].

РЕВОЛЮЦИИ *ОНЛАЙН*, КОТОРЫЕ ТАК И НЕ ПРОИЗОШЛИ

На сегодняшний день, по прошествии полутора лет с начала событий *Арабской весны*, первоначальный энтузиазм и ажиотаж вокруг социальных сетевых сервисов как основной движущей силы революций на Ближнем Востоке и в Северной Африке поутихли как в глобальных СМИ, так и среди экспертов. В числе последних — исследователи Центра Беркмана по изучению интернета и общества при Гарвардском университете — одного из ведущих центров по изучению социальных сетей и новых интернет-сервисов: Этан Цукерман, Дана Бойд, Джиллиан Йорк, Майк Ананни и Бет Колеман. На скептических позициях также стоят отечественные исследователи, в числе которых нужно отдельно упомянуть эксперта ИМЭМО РАН Е. А. Степанову, посвятившую отдельное исследование роли ИКТ в *Арабской весне*[4].

Обобщенная позиция экспертных кругов РФ и Запада сводится к тому, что социальные сети не сыграли ведущей роли в событиях *Арабской весны*, они не были доминирующим каналом коммуникации оппозиционных сил и участников протестов. Вместе с тем они частично придали событиям в арабских странах ту скорость и динамику, которая застала врасплох их оппонентов — правительства и поддерживающие их силы. Как справедливо отметил на страницах газеты *Коммерсантъ* автор термина *твиттер-революция*, сотрудник Стэнфордского университета Евгений Морозов (Evgeny Morozov), без социальных сетей революции в арабских странах «однозначно произошли бы по-иному»[5].

Но можно ли утверждать, что социальные сети сыграли принципиальную и, главное, самостоятельную роль в развитии событий *Арабской весны*? На мой взгляд, такое утверждение неверно как минимум по следующим причинам:

1. Протестная деятельность по отношению к социальным сетевым сервисам носила преимущественно самодостаточный и независимый характер, а вот обратное утверждение неверно. События *Арабской весны* и, в меньшей степени, неудавшаяся попытка *революции онлайн* в Белоруссии в 2011 г. дают несколько оснований для такого вывода. Во-первых, протестная активность онлайн и реальные, уличные действия, сформировавшие революцию, разнятся по пику своей активности и не полностью совпадают во времени. Как отмечал бывший председатель правления Союза директоров ИТ России А. В. Коротков, «уличные акции в Египте продолжались и в отсутствие сколь бы то ни было значимого влияния интернет-коммуникаций». Зеркальный пример: в Сирии объявленные в *Facebook* дни гнева в 2011 г. не переходили в масштабные уличные акции, все изменилось лишь после произведенных властями арестов подростков, спровоцировавших массовые столкновения.

2. Протесты были и там, где активность в социальных сетях была близка к нулевой. Однако при этом протесты в тех государствах, где использование ИКТ было максимально активным, проходили по более мягкому сценарию. Некоторые эксперты считают такую корреляцию следствием *гуманизирующей* роли интернета. Однако в действительности причинно-следственная связь скорее носила обратный характер. Чем более развито государство в социально-экономическом отношении и чем либеральнее относится режим к свободе коммуникации, тем выше уровень проникновения ИКТ, включая социальные сети. Примеры Ливии и Йемена как государств, которые обладают весьма низкими показателями проникновения интернета даже по региональным меркам (менее 20%) и при

этом стали ареной весьма ожесточенных и массовых акций протеста, а потом и вооруженной борьбы, говорят сами за себя.

3. Социальные сети не были ни единственным, ни даже ключевым средством коммуникации и координации действий повстанцев. При этом, однако, они были основным средством популяризации их движений и публичного контакта с внешним миром — в отличие от спутникового телевидения, мобильной связи, СМС, мечетей и всех остальных площадок коммуникации. В египетских провинциях, равно как и в Каире, главной площадкой для координации действий протестующих и распространения их настроений были мечети, сразу по окончании пятничных намазов превращавшиеся в своеобразные командные пункты участников протестных движений. Точно так же ситуация обстояла и во всех странах региона с малозначительными нюансами.

4. Та же *рецептура* протестной онлайн-активности с акцентом на социальные сети, которая сопровождала и подкрепляла развитие событий в арабских странах, не привела к запуску аналогичного сценария в Беларуси. Хотя лидер оппозиционного «Движения будущего» Вячеслав Дианов уповает на технологии социальных сетей и микроблогов, акции его активистов за 2011 г. так и не вышли за рамки локальных. Это еще раз подтверждает тезис о том, что все решают не коммуникации сами по себе, а социально-политический фон и содержание процессов, развивающихся в той или иной стране. Оказавшись вне специфической среды Ближнего Востока и Магриба, где революции были подготовлены социально-политическими процессами, вызревавшими в течение десятилетий, отточенная технология координируемого через сети протеста дала сбой и утратила эффективность.

Кроме того, сами социальные сети в *Арабской весне* не проявили себя в качестве субъектов корпоративных интересов, подобных крупным транснациональным корпорациям (ТНК). Их руководство и менеджмент не пытались управлять протестной активностью или хотя бы направлять ее. Менеджер *Google* Ваиль Гоним [Wael Ghonim], названный СМИ «международным лицом египетской революции»[6], действовал сугубо как частное лицо, с 2010 г. развивая деятельность протестного сообщества (страница *We are all Khaled Said*) на платформе главного конкурента своего работодателя — *Facebook*. При этом г-н Гоним не координировал свою деятельность с представителями *Facebook*, хотя и выражал надежду встретиться с Марком Цукербергом, чтобы поблагодарить его за возможности, которые *Facebook* предоставила египтянам. Более того, свою деятельность в качестве интернет-активиста топ-менеджер *Google* на Ближнем Востоке поначалу осуществлял параллельно с исполнением своих обычных рабочих обязанностей в *Google*, ведя, по его собственному признанию, двойную жизнь. Эти факты зачастую упускаются из виду теми комментаторами, которые пытаются изображать *Арабскую весну* 2011–2012 гг. как искусственный и управляемый процесс, в той или иной мере спровоцированный гигантами ИТ-индустрии.

При этом любопытно, что подобные точки зрения озвучивали представители самых высших эшелонов российской власти. Так, 22 февраля 2011 г. президент России Д. А. Медведев в разгар протестов в Египте назвал происходящее сценарием, который «они раньше для нас готовили»[7]. Еще дальше пошел И. И. Сечин, на тот момент занимавший пост вице-премьера РФ, заявив в интервью *The Wall Street Journal*: «Надо пристальнее изучить происшедшее в Египте. Посмотреть, что делали в Египте, скажем, высокопоставленные руководители *Google*, какие там были манипуляции с энергией народа»[8]. Такая интерпретация событий *Арабской весны* может служить тревожным признаком, сигнализирующим о непонимании либо игнорировании реальных роли и места социальных сетевых сервисов в общественно-политических процессах.

Рассмотренные выше ситуации и примеры позволяют утверждать, что на сегодня социальные сетевые сервисы как разновидность сетевых технологий, а также их аудитория как специфическая самоорганизующаяся общность едва ли представляют угрозу безопасности как на уровне отдельных государств, так и на международном уровне. Соответственно, дискуссия относительно того, как следует реагировать на вызовы безопасности, исходящие от социальных сетей, представляет собой не совсем корректную постановку вопроса. Этот посыл может быть актуален для политического руководства РФ при рассмотрении ими проблематики социальных сетей. Искать возможные вызовы безопасности в связи с развитием социальных сетевых сервисов стоит не в их технологии, замыслах их руководства и уж точно не в действиях их пользователей.

СТРАТЕГИЯ США В КИБЕРПРОСТРАНСТВЕ И СОЦИАЛЬНЫХ СЕТЯХ: ВЫЗОВЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

При анализе *Арабской весны*, как и ее своеобразных *афтершоков* за пределами Ближнего Востока, национальные государства и их правительства обычно изображаются пассивными *жертвами* технологий сетевых сервисов, активно используемых участниками протестов. Действия госструктур рассматриваются лишь в плоскости реакции на угрозы, якобы исходившие из интернета. Исключением являются США, которым часто приписывается роль тайного организатора и режиссера *Арабской весны*.

В России версия о причастности США к революциям на Ближнем Востоке через тайные каналы влияния, такие как социальные сети, находит благодатную почву по ряду причин. Играет роль недоверие к Вашингтону и традиционно сильные антиамериканские настроения среди представителей российской элиты. Кроме того, комбинация антиамериканизма и очередной вариации теории заговора дает определенные политические очки политическим движениям левого толка, позиции которых в России лишь усиливаются. Наконец, склонность видеть в глобальных процессах, подобных *Арабской весне*, срежиссированные кем-то геополитические сценарии во многом исходит от непонимания подлинных причин таких процессов и некорректной оценки их потенциального влияния на Россию и ее союзников. Пытаясь определить возможное направление угрозы, политический истеблишмент в первую очередь смотрит туда, куда более всего привык смотреть со времен СССР — по другую сторону Атлантики.

Однако серьезной критики версия о наличии в *Арабской весне* элемента управляемости и координации ее событий из Вашингтона не выдерживает. Первая официальная реакция руководства США на события в Тунисе и Египте весной 2011 г. продемонстрировала растерянность Белого Дома и склонность к осторожной, выжидательной тактике. Поначалу президент США Барак Обама высказывался в поддержку режима Хосни Мубарака как оплота стабильности на Ближнем Востоке и ключевого партнера Вашингтона в регионе. Этот пример весьма показателен на фоне того, что революции *Арабской весны* не состоялись или не достигли цели там, где свержение режимов в наибольшей степени отвечает интересам США — а именно в Иране, — однако поставило под удар многие стратегические интересы США на Ближнем Востоке.

Так, свержение Мубарака лишило Вашингтон давнего союзника, занимавшего благоприятные для Белого дома позиции по вопросам борьбы с исламским фундаментализмом, палестино-израильского урегулирования, противодействия международному терроризму. События в Ливии втянули Вашингтон в военную кампанию, совершенно не нужную президенту Обаме на фоне войны в Афганистане и приближения выборов. Волнения на Аравийском полуострове затронули *жизненно важные* для США вопросы: стабильность поставок нефти из Саудовской Аравии, лояльность режима саудитов, выступающего главным противовесом Ирану, а также беспрепятственное размещение американских военных баз на Аравийском полуострове. Чтобы отразить масштаб интересов США в отношениях с саудитами,

достаточно сказать, что в 2010 г. Эр-Рияд объявил о долгосрочном плане закупок вооружений у Вашингтона на общую сумму в 60 млрд долл.

Наконец, общим для арабского мира итогом революций стал прорыв наружу аккумулированного за предыдущее десятилетие антиамериканизма и антивестернизма. В 2012 г. Белый дом попал в незавидной ситуации, на словах приветствуя «торжество свободы» в Египте и Тунисе и с тревогой ожидая дальнейшего усиления исламистов, после того, как прошедшие парламентские выборы в основном подтвердили рост их влияния в этих странах.

В общем и целом тезис о причастности США к *Арабской весне* лишен серьезных оснований. В то же время его сторонники вполне справедливо фиксируют острый интерес Вашингтона к *возможности* осуществления подобных трансформаций в управляемом режиме. Однако не стоит забывать, что, поневоле играя роль *объекта*, ощущающего на себе последствия развития ИКТ, государства в то же время являются и *субъектом*, который пытается освоить эти возможности и технологии (включая технологии сетевых сервисов) и превратить их в инструмент реализации своего политического курса.

Возможности социальных сетевых сервисов в социально-политическом, военном и иных аспектах не могут не привлекать Соединенные Штаты, которые всегда играли особую роль в развитии интернета. Являясь создателями Сети и сохраняя частичный контроль над корневыми DNS-серверами через ICANN[9], США сохраняют определенную преемственность своей политики. Вашингтон демонстрирует элементы *миссионерского* подхода к вопросам, связанным с интернетом, в частности продвижению свободы слова в Сети и обеспечению беспрепятственного доступа к ней населения каждой из стран. Даже тот факт, что технологии социальных сетей вдруг преподнесли своей родине неприятный сюрприз, поставив под удар ее интересы на Ближнем Востоке, не влияет на фундаментальные подходы Белого дома к данным вопросам. Хотя политика Вашингтона в области киберпространства выходит далеко за рамки тематики социальных сетевых сервисов, ее анализ все же необходим, так как отдельные грани проблемы (подобные социальным сетям в контексте безопасности) нельзя рассматривать, не видя общей картины.

Своеобразной *презентацией* американского курса в отношении интернета на высоком уровне можно считать выступления Госсекретаря США Хиллари Клинтон по проблематике интернет-пространства, которые состоялись дважды, с интервалом чуть больше года — 21 января 2010 г. и 15 февраля 2011 г., всегда порождая немалый резонанс в СМИ и экспертном сообществе. Наибольший интерес представляет вторая речь «Интернет, за и против: выбор и вызовы в мире, связанном глобальной сетью». Во-первых, в ней нашли комплексное отражение события *Арабской весны*, по ключевым аспектам которой, включая роль ИКТ, администрация Обамы до этого давала лишь разрозненные и хаотичные комментарии, за которыми не было видно целостной позиции. Во-вторых, озвученные в выступлении г-жи Клинтон инициативы простираются далеко за рамки президентского срока Барака Обамы, что свидетельствует о серьезности курса Белого дома. В-третьих, в отличие от 2010 г. февральская речь оказалась весьма насыщена анонсами конкретных программ и проектов, в значительной степени завязанных на социальные сервисы и родственные им технологии.

Кроме того, взгляды Белого дома на развитие киберпространства уже в полной мере находят отражение в доктринальных документах американских ведомств. В числе последних следует упомянуть прежде всего Международную стратегию по действиям в киберпространстве [International Strategy for Cyberspace], опубликованную Белым домом 16 мая 2011 г. Ее своеобразным логическим развитием в военной плоскости стала Стратегия Министерства обороны по действиям в киберпространстве [Department of Defense Strategy for Operating in Cyberspace], частично рассекреченная в июне 2011 г. В совокупности с рядом крупных проектов в области киберпространства, о которых прессе стало известно в мае-июле

2011 г., принятие киберстратегий позволяет говорить о том, что проблематика интернета выходит на принципиально новый уровень в повестке Белого дома — и в первую очередь в плоскости безопасности. Можно выделить несколько принципов, на которых опирается нынешнее «признание киберпространства»[10] на высшем уровне и которые напрямую затрагивают социальные сетевые сервисы, хотя и не ограничиваются ими.

В первую очередь речь идет о закреплении и индоктринации курса Вашингтона на «глобальную войну с цензурой в интернете»[11]. Свобода в интернете стала идеологическим стержнем речи Госсекретаря и доминирующей идеологемой Вашингтона в отношении киберпространства в целом[12]. В плане предлагаемых лозунгов и ценностей Соединенные Штаты не слишком выделяются из ряда других государств, преимущественно членов ЕС, обладающих развитым ИКТ-сектором. В частности, такие страны, как Эстония, Греция, Финляндия, уже в течение нескольких лет признают доступ в интернет неотъемлемым правом человека, выступая против каких-либо его ограничений, включая цензуру, а не так давно этот тезис получил внушительную поддержку и на международном уровне. 7 июня 2011 г. был опубликован доклад ООН, в котором признается в качестве одного из неотъемлемых право на доступ в интернет[13]. От положений международной киберстратегии Вашингтона данный перечень отличает лишь отсутствие в нем прямой увязки права на доступ в интернет с демократическими ценностями.

Подход Вашингтона можно было бы рассматривать в сугубо положительном ключе, несмотря даже на характерное для США стремление увязывать развитие ИКТ со становлением демократических институтов. Но, как известно, дьявол кроется в деталях. Разделяя общепринятые ценности и преследуя близкие многим государствам цели политики в отношении интернета, США берут на себя чрезмерно амбициозную роль и опасно раздвигают рамки допустимых мер по реализации этой политики. Так, потенциальные риски для международной безопасности представляет принцип экстерриториальности борьбы США за свободу и безопасность в киберпространстве. Его чеканная формулировка прозвучала в февральской речи Хиллари Клинтон: «США защищают свободу [общения в интернете] повсюду и призывают все остальные страны к тому же»[14]. Более того, Госсекретарь не преминула привести список государств — «врагов свободного интернета», на которые будут в первую очередь направлены инициативы ее ведомства. Любопытно, что в список, включающий Сирию, Иран, Китай, Кубу и Вьетнам, попали две страны из бывшего перечня государств-изгоев [rogue states], актуального при администрации Джорджа Буша-младшего. Эта деталь высвечивает определенную параллель между риторикой г-жи Клинтон и догмой Буша-младшего о «демократии на марше». В обоих случаях в основе лежит видение США как проводника тех или иных универсальных ценностей, имеющего право на односторонние превентивные действия в отношении государств, их не разделяющих.

Однако доктринальные документы могут оказывать реальное влияние на ситуацию в области безопасности лишь в том случае, когда их положения и принципы получают практическое наполнение и отражаются в конкретных проектах и инициативах. Реализация курса, заложенного в американских программных стратегиях и выступлениях, является *лакмусовой бумажкой*, определяющей, будет ли реализован тот потенциал влияния на международную безопасность, который в них заложен.

На сегодняшний день можно выделить две группы проектов, которые позволяют утвердительно ответить на этот вопрос. В центре этих проектов оказываются технологии мобильной связи, а также инструменты Web 2.0, прежде всего социальные сетевые сервисы. К сожалению, в обоих случаях уместно говорить о том, что инициативы Вашингтона несут в себе значительный негативный потенциал для международной безопасности.

Во-первых, речь идет о проектах Госдепартамента по созданию так называемых *теневых* систем мобильной и интернет-связи для поддержки оппозиции в авторитарных государствах. Информация о них появилась в июне 2011 г., опять же

в контексте *Арабской весны,* однако соответствующие планы ведомства были четко обозначены еще в выступлении Госсекретаря Хиллари Клинтон в феврале 2011 г. Одна из разработок связана с усовершенствованием технологии Bluetooth, которое позволит создать систему автоматизированного распространения текста и мультимедийного контента по скрытой сети из «доверенных пользователей»[15]. Еще один проект, также находящийся в стадии реализации, предполагает строительство автономных сетей мобильной связи, способных обеспечивать покрытие на территории, не подконтрольной США и их союзникам. Отрабатывая подобную технологию на своих военных базах в Афганистане, США заимствуют опыт жителей КНДР, использующих китайские приграничные сотовые вышки для передачи сообщений через мобильные телефоны[16].

Не менее активно развиваются проекты, призванные обеспечить оппозиции возможность доступа в интернет в обход контролируемых государством сетей. Наиболее примечательным из них является так называемый *интернет в чемоданчике*, предполагающий создание компактного устройства, которое можно незаметно ввезти в страну и развернуть с помощью него сеть с выходом в интернет и довольно обширным покрытием. По словам представителей интернациональной команды разработчиков проекта из 12 стран, речь идет об «изолированной сетевой инфраструктуре, которую невозможно контролировать, нельзя отследить и очень трудно уничтожить»[17]. Систему также предполагается снабдить технологией, мешающей идентификации пользователя. *Чемоданчик* должен позволить оппозиции в авторитарных государствах координировать свои действия онлайн и поддерживать связь с миром даже в условиях полной блокировки интернета государством. Госдепартамент не скрывает, что основной задачей тех групп и движений, которым планируется предоставлять доступ к данной технологии, является «подрыв репрессивных режимов»[18].

Такая риторика указывает на то, что в Белом доме ищут возможность повторить *Арабскую весну* в управляемом варианте — в нужной стране и в нужное время, причем в основном с помощью интернета и мобильной связи. Прежде всего такая тактика способствует дестабилизации обстановки в тех странах, где она применяется. Например, в Иране, который является первоочередной мишенью Госдепартамента в связи с эскалацией кризиса вокруг ядерной программы Тегерана, каждый всплеск протестов приводил к новому витку репрессий и кровопролитию, приближая ситуацию к опасному тупику и социальному взрыву. Режимы, которые Белый дом хочет *подорвать* в первую очередь, не похожи на режимы Бен Али в Тунисе и даже Хосни Мубарака в Египте — по уровню авторитаризма и готовности применять силовой ресурс в целях самосохранения они стоят куда ближе к свергнутому режиму Муаммара Каддафи в Ливии. Все, чего можно достичь с помощью *чемоданчика* в Иране, Китае, Туркмении и прочих нелюбимых Вашингтоном *автократиях*, это спровоцировать новую волну насилия с неясным исходом, но никак не добиться торжества свобод, о которых говорит г-жа Клинтон.

Ярким примером служит развитие событий в Сирии, где противостояние повстанцев и режима Башара Асада, начавшееся с мирных акций протеста, к середине 2012 г. вылилось в полномасштабную гражданскую войну. Хотя США не использовали против режима Асада секретные ИКТ-разработки, предпочитая традиционные методы влияния на ход внутреннего конфликта (в том числе инструктаж повстанцев и массированную информационную поддержку по всему спектру от официальной дипломатической риторики до тех же социальных сетей), важен сам итог такого подхода. Ситуация в Сирии в целом не лежит на совести Белого дома, но вклад в эскалацию насилия и расширение его масштабов, по-видимому, все же был сделан. Применение более изощренных инструментов, подобных описанным проектам в области интернет-технологий, ничем не изменило бы ситуацию. То же будет верно, если говорить о гипотетических вариантах применения *интернет-чемоданчика* для подогрева протестных настроений в Иране и любой другой стране.

Еще больше вопросов вызывают инициативы Пентагона, получившие название *SMISC* (Социальные медиа в стратегической коммуникации). В рамках проекта делается фокус исключительно на сетевые социальные сервисы; целью его является использование социальных сетей, видеохостингов и микроблогов в целях разведки, контрразведки и ведения информационно-пропагандистской борьбы. Проект предполагает использование социальных сетей напрямую в военных целях, информация о нем появилась в открытых источниках в июле 2011 г., вскоре после частичного обнародования военной киберстратегии Пентагона. Достаточно изощренная с технологической точки зрения концепция предполагает разработку специальной программы, которая, будучи неким образом развернута в крупнейших сетевых сервисах (*Facebook, Twitter, YouTube*), позволит осуществлять широкий спектр задач, де-факто лежащих в плоскости военной разведки. В числе прочего программа должна позволять военным и спецслужбам «противодействовать враждебным кампаниям влияния с помощью контрсообщений, отслеживать враждебную по отношению к США пропаганду и помогать вести контрпропаганду»[19].

Система, разработка которой является целью гранта Управления перспективных научно-исследовательских разработок Минобороны США (более известна как DARPA), ориентирована на чрезвычайно широкий круг задач. В частности, в ее функции входят обнаружение, классификация и анализ появляющихся в социальных сетях сообщений на предмет наличия в них информации, имеющей ценность для военной разведки или представляющей опасность для США. К такой информации относятся сведения о морально-психологическом состоянии военнослужащих и различных групп населения отдельных стран и регионов, общественные тенденции, новые идеи или планирующиеся события, а также факты распространения недружественной пропаганды и дезинформации[20]. Несмотря на то что проект можно назвать технологически прогрессивным и даже задающим новые стандарты обработки информации в сетевых сервисах, его влияние на международную безопасность и развитие интернета следует признать деструктивным по целому ряду соображений.

Прежде всего вызывают серьезные сомнения надежность и достоверность информации, получаемой в результате подобного проекта. Ставящиеся задачи исключительно сложны даже при использовании традиционных методов разведывательной и контрпропагандистской деятельности. При осуществлении же таких задач в киберпространстве на порядок вырастает риск дезинформации, информационных помех и неверной интерпретации полученных данных. Разведывательная деятельность Пентагона через социальные сети может быть достаточно легко *обессмыслена* путем массового создания в социальных сетях бот-акканутов военнослужащих, и это лишь одно из возможных решений.

Подобное препятствие останется проблемой самих Соединенных Штатов, но лишь до тех пор, пока на основе этих данных не будут приниматься военно-стратегические решения. Недостаточно тщательный анализ данных из соцсетей в этом случае может стать причиной искаженных, неверных оценок военными и спецслужбами США ситуации в других странах, протекающих в их обществах процессов, отношения их социальных групп к Соединенным Штатам. В случае дипломатических кризисов и конфликтных ситуаций подобная информация может стать одним из факторов, толкающих руководство США к жесткой реакции, эскалации кризиса — словом, привести к ошибке в стратегических решениях, что несомненно отразится на международной безопасности.

Второй негативной стороной *SMISC* является то, что инициативы Пентагона не могут не беспокоить другие государства и не провоцировать их ответную реакцию. Есть все основания полагать, что эта реакция будет носить весьма негативный характер как в смысле международной безопасности, так и в плане продвижения свободы в интернете, за которое столь активно выступает Белый дом. Своей политикой США в лице Пентагона дают крупный козырь в руки изоляционистским режимам и вообще сторонникам управляемого и жестко регулируемого

интернета. В этом смысле стоит согласиться с экспертом российского интернет-сообщества А. Сидоренко, по словам которого «резкая политизация интернета играет на руку как раз авторитарным режимам, которые стремятся интернет плотно контролировать»[21].

Наконец, инициатива Пентагона, получив широкую огласку, бьет по самим социальным сетям, представляя их как потенциальные инструменты тайных военных программ. Это может стать дополнительным фактором, под действием которого авторитарные режимы вновь усилят давление на компании, обеспечивающие деятельность социальных сетевых сервисов на их территории. В частности, такие тенденции можно прогнозировать в Китае, Иране и даже в России, где существуют мощные лоббистские группы, выступающие за более плотный контроль над интернет-коммуникациями и, одновременно, видящие в США едва ли не ключевой источник угроз национальной безопасности РФ. Хотя логика этих групп, преимущественно состоящих из высокопоставленных представителей силовых структур, страдает изъянами, их влияние бесспорно — его иллюстрацией может служить инициатива ФСБ о запрете сервисов *Skype, Hotmail* и *Gmail*, от которой так и не отказались с тех пор, как в 2010 г. она впервые была озвучена.

Таким образом, Россия также может пострадать от программ Пентагона, заплатив за вынужденные меры по обеспечению безопасности национального сегмента сети торможением его развития. По мнению экспертов, *SMISC* способны представлять реальные риски для национальной безопасности России. Как отметил главный редактор журнала *Национальная оборона* И.Ю. Коротченко, данные, публикуемые в российских сетях (например, в ныне уже неактивном сервисе «место службы» на *Одноклассниках* и многих других подобных ресурсах) представляют богатый источник развединформации[22].

Инициативы Госдепартамента и Пентагона делают курс США в отношении киберпространства в значительной степени антиконструктивным. При этом под удар попадают те самые ценности, которые США стремятся продвигать и поддерживать — свобода в интернете (включая свободу доступа), отсутствие цензуры и жесткого контроля со стороны государства, единство и гармоничное развитие киберпространства, беспрепятственное развитие интернет-компаний и технологий.

Американская доктрина в отношении интернета стоит на прогрессивном фундаменте, однако воплощается при помощи не совсем адекватного инструментария и с идеологическими перекосами. Пытаясь реагировать на угрозы, исходящие из киберпространства, Белый дом придает функцию военных и политических инструментов технологиям, которым она изначально не присуща. Социальные сервисы, в отличие от ARPANET и многих других достижений ИКТ, изначально развивались как общедоступное трансграничное средство общения. Использование их в тайных разведывательных и тем более военных целях во многом противоречит тем качествам, которые выдвинули их на авансцену развития сегодняшнего глобального интернет-сообщества.

Неосмотрительные инициативы Вашингтона, таким образом, подстегивают процесс, который в случае своего дальнейшего развития может вылиться в полномасштабную *милитаризацию киберпространства*, способную стать одной из серьезных международных проблем наряду с милитаризацией космоса. Текущие тенденции свидетельствуют о том, что США стремятся не столько к тому, чтобы остановить этот процесс, сколько к тому, чтобы обеспечить себе позицию лидера в данном направлении. Притом что социальные сетевые сервисы оказываются на острие стратегий Белого дома, их применение в описанных выше целях действительно претендует на статус нового серьезного вызова международной безопасности, хотя вне контекста государственной политики социальные сервисы, повторимся, такого вызовы не несут.

СОЦИАЛЬНЫЕ СЕТИ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ: ЗА РАМКАМИ *ТВИТТЕР-РЕВОЛЮЦИЙ* И МЕЖДУНАРОДНОЙ ПОВЕСТКИ ДНЯ

Разумеется, значение соцсетей в современном обществе не исчерпывается ретрансляцией и поддержанием социальных волнений и протестной активности, даже если рассматривать их сугубо применительно к сфере международной и национальной безопасности. Использование социальных сетевых сервисов в интересах национальной и международной безопасности возможно, и оно уже развивается сразу по многим направлениям.

1. Первым из них являются различные разновидности *краудсорсинга* (от англ. crowdsourcing) — явления, получившего свое наименование в 2006 г. в статье Джэка Хауи (Jeff Howe) в журнале *Wired*[23]. Краудсорсинг означает передачу каких-либо действий, работ и функций вообще неопределенному внешнему кругу лиц на неоплачиваемой основе. За прошедшие несколько лет с момента своего создания краудсорсинг онлайн получил широкое распространение не только на Западе, но и во многих других регионах и странах, включая Россию.

За последнее время одним из наиболее ярких и успешных проектов подобного рода в России стала «Карта помощи пострадавшим от пожаров», созданная в 2010 г. известным интернет-активистом и теоретиком Григорием Асмоловым (Gregory Asmolov). Это онлайн-сообщество функционирует на базе специальной платформы *Ushahidi*, позволяющей в рамках единого сервиса агрегировать и ретранслировать информацию с мобильных телефонов (через СМС-сообщения), электронной почты, а также обычных веб-сайтов. «Карта» показала себя как весьма эффективная информационная сеть, своеобразный узел, на который оперативно поступала информация о текущих событиях по различным каналам. Сама платформа была создана в 2008 г. с целью сбора и обмена информацией о случаях насилия после президентских выборов в Кении. Проекты на платформе *Ushahidi* помогали специальным службам спасать людей после землетрясений в Чили и на Гаити в 2010 г. Схожей технологией интерактивных карт *OpenStreetMaps* также успешно пользовались на Гаити американские спасатели, о чем упоминала Госсекретарь США Хиллари Клинтон в своей речи о свободе в интернете 21 января 2010 г.[24].

Словом, целесообразность сотрудничества государства с такими сообществами достаточно очевидна, однако в России такое взаимодействие сегодня практически отсутствует. Как отмечал г-н Асмолов на встрече Президента РФ с представителями интернет-сообщества, «мы видим все больше и больше примеров, когда сетевое общество может быть равноценным партнером государства в решении тех или иных социальных проблем»[25]. Но одновременно создатель «Карты помощи» признал, что контакты с Министерством чрезвычайных ситуаций (МЧС) РФ были установлены лишь по инициативе самих представителей комьюнити, а помощи от Министерства на тот момент фактически так и не последовало. Как отмечает соавтор проектов г-на Асмолова А. Сидоренко, МЧС демонстрирует собой образец «полного провала во взаимодействии с сетевыми технологиями».

Несмотря на радикальность такой оценки, наличие проблем взаимодействия нельзя не признать. В частности, власти достаточно неохотно идут на контакт с сообществами, деятельность которых направлена на защиту общественной безопасности в частности на борьбу с преступностью и пресечение незаконной деятельности. Таким краудсорсинг-проектом в РФ является сайт *Гдеказино.ру*, где также используется технология интерактивных карт для обмена данными об объектах азартного бизнеса. Проект оказался востребован правоохранительными органами, лишь когда президент РФ Д. А. Медведев лично отдал распоряжение российскому генпрокурору Юрию Чайке провести проверки по адресам казино, указанных на сайте[26].

По ряду перечисленных направлений государство не только не выступает с уже назревшими инициативами, но и игнорирует те предложения и идеи, которые поступают из общественной и экспертной среды. На встрече Президента России

Д. А. Медведева с представителями российского интернет-сообщества 19 апреля 2011 г. предложения о налаживании взаимодействия властных структур с сетевыми *краудсорс-комьюнити* встретили положительный отзыв президента, однако не получили реального развития[27].

Как следует из слов самого Д. А. Медведева на упомянутой встрече, на сегодня внимание к сетевым сообществам у государственных структур возникает в отдельных случаях, не на системном уровне, не в отлаженном рабочем режиме.

По отдельным направлениям взаимодействие госструктур с проектами формата краудсорсинга уже зарождается на уровне региональных органов власти. Так, по словам А. Сидоренко, правительство Пермского края использует данные краудсорсинга, например, таких ресурсов, как *Streetjournal.ru* и *Roards.teron.ru*. Определенный обратный отклик со стороны государственных органов вызывают проекты блогера А. А. Навального *Rospil.info* и *Rosyama.ru*, которые по некоторым параметрам можно причислить к краудсорсингу. Кроме того, в последнее время определенный интерес к краудсорсингу отмечается со сторону научно-аналитических институтов, близких к правительству. Как отметил Григорий Асмолов, автор ряда краудсорсинг-проектов, «позитивным примером является то, что при поддержке ИНСОР[28] разрабатывается платформа для взаимопомощи в кризисных ситуациях *Виртуальная рында — атлас помощи*».

Однако эти тенденции пока не распространяются на вопросы обеспечения безопасности в силу ряда причин. Во-первых, играют роль объективные ограничения, такие как секретный характер деятельности многих госструктур в сфере безопасности, а также централизованный характер обработки информации и принятия решений в них, весьма далекий от *grass-roots* уровня краудсорсинга. Однако не менее важны изъяны в работе российских госорганов, ответственных за обеспечение безопасности, и в первую очередь силовых структур. Речь в том числе идет об их традиционной закрытости, определенном консерватизме и запаздывающем освоении новых форматов взаимодействия с общественными структурами, а также вытекающем отсюда недоверии к этим структурам и используемым ими технологиям.

Между тем необходимость укрепления связей и наращивания сотрудничества госструктур с интернет-сообществом из числа опрошенных мной экспертов отметили представители ряда российских федеральных ведомств и самого интернет-сообщества. Таким образом, основная рекомендация для органов государственной власти РФ должна сводиться к необходимости преодоления:

а) инертности и пассивности органов, отвечающих за безопасность, в отношении социальных сервисов и наполняющих их сообществ пользователей как потенциальных партнеров в исполнении своих функций;

б) *ручного управления* взаимодействием госструктур с интернет-сообществом, препятствующего налаживанию устойчивого двустороннего сотрудничества и укоренению его системного характера.

2. Другая сфера применения социальных онлайн-сервисов не столь однозначна и даже противоречива в плане влияния на безопасность. Речь идет о социальных сервисах как инструменте формирования информационной картины событий и общественного мнения. Обычно принято говорить как о традиционных СМИ, так и об интернет-медиа (к числу которых принадлежат и соцсети), используя негативный контекст *информационного оружия*. Однако опыт РФ и других стран показывает, что эта медаль также имеет свою вторую сторону, и социальные сетевые сервисы могут быть как *мечом*, так и *щитом* в информационном противоборстве.

Первым классическим примером применения социальных медиа в качестве *оборонительного средства* принято считать действия израильских блогеров во время Второй Ливанской войны. В 2006 г. небольшая, но чрезвычайно активная израильская блогосфера в основном отражала шквал международной критики, который

обрушился на руководство страны не только из арабского мира, но и из многих западных стран и ООН, особенно после печально известного эпизода бомбардировки г. Каны израильскими ВВС в ночь на 30 июля 2006 г., унесшего жизни 28 мирных жителей. Усилиями блогеров удалось опровергнуть намеренно завышенное Хезболлой в 2 раза число жертв бомбардировки; также во многом благодаря израильской блогосфере был установлен постановочный характер фотографий с места бомбардировки, которые ранее были растиражированы такими ведущими СМИ, как *Reuters.* Наконец, израильские блогеры активно защищали свою страну и в других национальных сегментах блогосферы, включая российский, что в определенной степени повлияло на отношение общественности в России к действиям израильской стороны в конфликте.

Для России не менее ярким примером активности онлайн-сообществ в условиях агрессивной информационной кампании стала *Пятидневная война* 2008 г. Во время повального осуждения действий РФ на международном уровне блогосфера стала одной из немногих площадок, на которых активно отстаивалась альтернативная версия событий, не столь негативная для имиджа РФ. По сути, именно блогосфера не позволила российской стороне *всухую* проиграть информационную битву в августе 2008 г. Российским блогерам и сочувствующим активистам из-за рубежа удалось предпринять ряд действий, которые хотя и не переломили общую картину конфликта в Сети и глобальных СМИ, однако внесли в нее ряд корректив.

Так, коллективный флэшмоб российских блогеров привел к убедительной победе пророссийской позиции в голосовании на сайте CNN — на вопрос «Оправданы ли действия России в Грузии?» утвердительно ответили 92%, или 273,9 тыс. человек[29]. Благодаря блогерам скандальную известность получил новостной выпуск *Fox News*, в котором ведущий не дал беженкам из Южной Осетии (Аманде Кокоевой и Лоре Тедеевой-Коревиски) высказать в эфире обективную точку зрения. Наконец, определенный вклад в укрепление доверия к российской точке зрения внесли блоги очевидцев с места событий, включая военных специалистов, журналистов и просто жителей Южной Осетии.

На фоне активности рядовых граждан в блоговых, микроблоговых сервисах и социальных сетях (*Facebook, ВКонтакте*) реакция официального Кремля и российских СМИ выглядела удручающе запоздалой и неубедительной, о чем неоднократно говорилось впоследствии. Единственным мероприятием в сфере информационной борьбы стал пресс-тур для зарубежных журналистов по Цхинвали, состоявшийся 12 августа 2008 г., после окончания боевых действий, когда *мейнстримная* антироссийская точка зрения на конфликт уже закрепилась в массовом сознании жителей зарубежных государств.

Однако Минобороны РФ вынесло из этих событий определенные уроки. В январе 2012 г. в открытом доступе появился документ ведомства под названием «Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве»[30]. Представляя собой, по сути, новый доктринальный продукт Минобороны в области информационного противоборства, «Концептуальные взгляды…» уделяют большое внимание вопросам информационного освещения конфликтов и влияния на формирование общественного мнения. Так, в рамках задач по сдерживанию и предотвращению конфликтов предполагается «публично, объективно и своевременно разъяснять мировой общественности причины и истоки конфликта». Отмечается, что такие меры позволяют создать в «глобальном информационном пространстве» климат, удерживающий организаторов конфликта от его дальнейшей эскалации.

Не ограничиваясь этим пунктом, авторы документа также отмечают роль информационной работы непосредственно *в ходе* конфликта. В частности, постоянное информирование СМИ и работа с общественным мнением в ходе конфликтной ситуации призваны «эффективнее влиять на ее деэскалационное развитие». В целом, несмотря на громоздкость формулировок, в документе вполне четко и здраво отмечаются задачи информационного обеспечения деятельности воору-

женных сил. Появление подобных наработок говорит о том, что российские силовые структуры начали активно восполнять тот пробел, который существовал ранее в теоретическом осмыслении ИКТ и глобальных СМИ применительно к спектру их прямых ведомственных задач.

3. Еще одна сфера применения соцсетей, довольно близкая к краудсорсингу, — использование подобных сервисов в качестве систем экстренного оповещения о чрезвычайных ситуациях, катастрофах и различных угрозах. Пионерами в данном направлении являются США: в апреле 2011 г. стало известно о том, что Министерство национальной безопасности планирует использовать популярные социальные сети, в том числе *Twitter* и *Facebook,* для оповещения граждан страны о террористических угрозах. Более того, по данным СМИ, в будущем система может вовсе заменить традиционную для страны цветовую шкалу террористической угрозы.

Другой пример дала полиция австралийского штата Квинсленд в декабре 2010 г. — январе 2011 г. Во время мощнейшего наводнения и вызванной им массовой эвакуации жителей стандартная система оповещения стала давать сбои из-за возросшего потока запросов на сайты госучреждений и частичного отключения мобильной связи. В этой ситуации было принято решение о дублирующем оповещении населения через страницы на *Facebook* и *Twitter* полицией Квинсленда, а также службой информации аэропорта столицы штата г. Брисбена. Идея дала результат — активность пользователей не повлияла на работу серверов социальных сетей и позволила частично разгрузить сайты упомянутых госучреждений. Наконец, получать информацию из социальных сетей в кризисных ситуациях стремятся сами пользователи — в Японии сразу после цунами 11 марта 2011 г. поток *твитов* из Токио возрос многократно, превысив 1200 сообщений в час[31].

Нандан ***Унникришнан****, директор по евразийским исследованиям, старший научный сотрудник Исследовательского фонда Observer, Рахул Пракаш, младший научный сотрудник, Институт исследований безопасности Исследовательского фонда Observer — по электронной почте из Дели:* В августе 2012 г. мы в очередной раз стали свидетелями того, как интернет и социальные сети могут быть использованы для создания паники и дезорганизации повседневной жизни в отдельно взятой стране. Распространение *фейковых* фото- и видеоматериалов и искаженных слухов об антимусульманских погромах в Ассаме и Мьянме и реакции на них спровоцировало массовое бегство представителей определенных этноконфессиональных групп из ряда индийских городов. Учитывая культурное, этническое и конфессиональное многообразие Индии, использование естественного потенциала для социальных волнений представляет серьезный предмет озабоченности для властей. Наиболее яркий эпизод недавних событий, когда до 300 тыс. человек бежали из Бангалора после распространения в социальных сетях сообщений о скором начале погромов, служит примером того, как интернет может использоваться для подрыва социальной гармонии. Правительству необходимо выработать политику и стратегии предотвращения подобных ситуаций. Как бы то ни было, делать это следует, не выходя за рамки ключевых положений индийской конституции — включая нормы о свободе слова и самовыражения. Соответственно, полная блокировка сайтов по образцу китайской модели для Индии неприемлема.

Таким образом, в информационно развитых странах и органы власти, и само общество начинают уделять внимание социальным сетям как источнику и ретранслятору информации в тех ситуациях и направлениях деятельности, которые напрямую связаны с обеспечением безопасности. В будущем эта тенденция, без сомнения, будет набирать силу по мере адаптации госструктур к прогрессу ИКТ.

Что касается России, то на этом поле какой-либо целенаправленной активности российских госструктур пока не наблюдается. Так, принятые Госдумой РФ 22 апреля 2011 г. поправки в закон «О противодействии терроризму» вводят цветовую шкалу террористической угрозы, но не предполагают использования соцсетей для информирования населения, в отличие от американского законопроекта. Возможно, причина лежит в более низкой по сравнению с США степенью проникновения данных сервисов в РФ — около 20% населения по сравнению с 45% в Штатах[32]. Но и теракты в России происходят не в пример чаще, даже если не брать в расчет Северо-Кавказский федеральный округ с крайне низким уровнем проникновения интернета.

Другим свидетельством слабого прогресса российских госорганов в освоении ИКТ для задач экстренного оповещения стали катастрофические наводнения на Кубани в июле 2012 г., когда оповещения не было вовсе. Представляется, что деятельность госорганов в этой области должна получить импульс критики со стороны гражданского общества, а также импульс идей и предложений от частного сектора, чтобы ситуация начала выправляться. Для этого, однако, необходима хотя бы минимальная терпимость властей к критике и готовность к восприятию частных инициатив, о чем затруднительно говорить в случае с Крымском.

РАЗВИТИЕ СОЦИАЛЬНЫХ СЕТЕЙ В РФ — ПРОБЛЕМЫ И ЗАДАЧИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

В дискуссии о роли соцсетей в контексте безопасности принципиально важен вопрос идентификаций их пользователей. По словам одного из ведущих российских экспертов в области информационного права, решение этой проблемы является «основной на сегодня задачей, стоящей перед Россией и другими странами в сфере управления интернетом». При этом идентификация в соцсетях неразрывно связана с общей проблемой идентификации пользователей в интернете. Ее актуальность частично вытекает из уже упомянутых выше примеров, таких как случай *сирийской блогерши*, хотя он и не описывает все потенциальные риски, связанные с так называемой активной анонимностью в Сети. Ситуация, когда пользователь может с легкостью обойти существующие средства идентификации, открывает возможности для кибермошенничества, размещения общественно опасного и неприемлемого контента, проявлений экстремизма и социальной агрессии онлайн.

Уже сейчас эта тема включается в рабочую повестку российских структур, в ведении которых находятся вопросы национальной безопасности. Согласно нашему источнику в СБ РФ, «в последнее время в повестке Совета стало уделяться внимание проблеме терроризма в социальных сетях». Корни проблемы во многом уходят в максимально свободный (до июня 2011 г.) режим регистрации пользователей *ВКонтакте*. До сих пор эта социальная сеть выдает сотни и тысячи результатов в поиске страниц, групп, заметок и видео с призывами к «джихаду против неверных», построению «имарата кавказ», бунту мусульманского населения РФ против федералов и т.д.

В свою очередь, такое обилие неприемлемого контента объясняется тем, установить личность пользователя, выложившего его в сеть, практически невозможно. Отсюда и следует огромное количество профилей «муджахидов», «воинов ислама», немыслимых для *Facebook*, *LinkedIn, Google+*. Даже наполняя подобный профиль определенной личной информацией, пользователи знают, что останутся безнаказанными, если только лично ими не заинтересуется ФСБ (что крайне

маловероятно по понятной причине — за всеми не уследишь). Кроме того, 15 марта 2011 г. *ВКонтакте* удалось выиграть в суде во многом прецедентное дело, связанное с размещением в сети контента, нарушающего права правообладателя[33]. Однако согласие суда с доводами представителей социальной сети, что ответственность за размещаемые материалы лежит на пользователях, лишь дает зеленый свет дальнейшим нарушениям подобного рода со стороны *де-факто анонимных* пользователей.

Решения проблемы варьируются в зависимости от различных технологических путей их реализации. Наивысшая надежность идентификации в теории может быть достигнута при использовании программ и технологий, которые предполагают шифрование (кодирование) и снабжение цифровой подписью той информации, которой обмениваются пользователи. Классическим примером таких программ служит система PGP (*англ.* Pretty Good Privacy), разработку которой начал в 1991 г. небезызвестный американский программист Филипп Циммерман (Philip Zimmermann). Уже в первой версии программы, основанной на принципе *Сети доверия* [Network of Trust], предполагался механизм открытых и закрытых ключей, а также цифровых сертификатов, взаимное подтверждение которых и обмен ключами формировали *Сеть доверия* между пользователями, куда не мог вклиниться посторонний или злоумышленник.

Однако сегодня такие программы заведомо неприемлемы для коммерчески ориентированных крупных сетевых сервисов, соревнующихся друг с другом в простоте и дружественности пользовательского интерфейса, а также в легкости расширения круга контактов каждого из пользователей. Более того, по мнению эксперта МГИМО (У) МИД РФ В. В. Каберника, проблематичными для социальных сетей могут стать и менее радикальные варианты, такие как перевод работы с данными сервисами в HTTPS, защищенное расширение протокола HTTP, поддерживающее шифрование вводимых данных. Так как ключевое значение в современных социальных сетях, как упоминалось выше, имеют ссылки на посторонний аудио- и видеоконтент, размещаемый в незащищенном HTTP, работа пользователей с ними будет существенно затруднена. Компромиссным вариантом, с точки зрения эксперта, мог бы стать перенос в HTTPS процедуры регистрации и авторизации пользователя в социальных сетях.

Сами социальные сети, по крайней мере в РФ, пытаются решать проблему идентификации пользователей исходя из собственной логики, далеко не всегда успешной. С 11 июля 2011 г. *ВКонтакте* ввела регистрацию пользователей по номерам мобильных телефонов, избрав компромиссный вариант между закрытой системой регистрации и открытой, имевшей место ранее. Привязка аккаунта к номеру сотового является вариантом идентификации, который довольно эффективен в том случае, когда все пользователи являются гражданами РФ, где мобильный номер (промежуточная ступень идентичности в данном случае) приобретается по паспорту. Но считать этот путь полностью успешным мешает трансграничность *ВКонтакте*, присущая любой крупной социальной сети. Как уже упоминалось, около 40 млн аккаунтов в сети Павла Дурова зарегистрированы за пределами РФ, а значит, их хозяева приобретают мобильные номера в соответствии с зарубежным законодательством. По данным на начало апреля 2011 г., *ВКонтакте* насчитывалось 16,5 млн аккаунтов пользователей из Украины[34], где мобильные номера не привязаны к документам, удостоверяющим личность владельца. В странах Европы, таких как Испания, мобильные номера вообще не закреплены за каким-либо конкретным провайдером сотовой связи. В результате, идентификация 30% пользователей соцсети оказывается фиктивной. Таким образом, подход, избранный *ВКонтакте*, должен дополняться решениями, которые покрывали бы упомянутые *серые зоны*.

В их числе можно упомянуть привязку аккаунта в соцсети к банковскому счету пользователя, вариантом которой можно считать распространение на социальные сети правил электронных платежных систем, таких как *PayPal, Webmoney, Яндекс.Деньги* и другие. Преимуществом такого решения стала бы высокая

надежность идентификации и ценность аккаунта в глазах пользователя (особенно если в Пользовательское соглашение с соцсетью будет включен пункт о заморозке определенной суммы на счете в случае нарушения его положений). В настоящее время можно выделить две уязвимых места в данной идее:

а) охват пользовательской аудитории в данном случае опять же будет неполным. По информации на март 2011 г., банковские счета имели лишь 47% россиян[35], хотя среди молодежи, которая составляет костяк аудитории социальных сетей, этот процент существенно выше. Кроме того, неясно, каким образом удастся выстроить сотрудничество социальных сетей с зарубежными банками, не ведущими деятельность в РФ;

б) увязка аккаунта с банковским счетом может встретить сопротивление как самих социальных сетей и всех стейкхолдеров данной отрасли, так и банков, которые попросту столкнутся с необходимостью обработки потока не нужной им информации.

Ожидать подвижек по второму пункту можно лишь при условии успешной и массовой коммерциализации услуг социальных сетей, ориентированной именно на их оплату с банковских счетов. Первые шаги в этом направлении в начале июля 2011 г. сделали две крупнейшие социальные сети РФ (*ВКонтакте* и *Одноклассники*), которые ввели возможность привязки оплаты платных услуг с карт банков-партнеров (вместо платных СМС)[36]. Ключевых вопроса здесь два: можно ли превратить такую *опцию* в *обязательство* и достаточны ли меры безопасности, применяемые для защиты вводимых пользователем банковских реквизитов. В плане безопасности предпочтителен путь *Одноклассников*, когда при регистрации пользователь работает в защищенной базе самого банка, уже после этого переходя в обычный интерфейс социальной сети. По сути, такая схема почти полностью укладывается в логику приводимых выше рекомендаций В. В. Каберника.

Но так или иначе перечисленные меры не решают проблемы идентификации пользователей полностью — для этого необходим комплексный подход, распространяющийся на все интернет-пространство. В РФ он пока отсутствует, так как не существует, во-первых, консенсуса относительно должной степени вмешательства государства в данную область; во-вторых, отсутствует единое видение этого подхода на техническом и юридическом уровнях. В данных условиях целесообразно тщательное и многоуровневое изучение зарубежного опыта, как положительного, так и негативного. Как отмечает известный российский эксперт в области информационного права, «сегодня отечественным органам власти необходим мониторинг наработок и решений других стран и международных организаций в данной области».

Между тем за рубежом наиболее интересные решения предлагают США, где в последние годы обсуждается идея введения *интернет-паспортов*, действие которых охватит не только социальные сервисы, но и всех пользователей Всемирной сети. В конце 2010 г. была впервые опубликована черновая версия Национальной стратегии достоверной идентификации в киберпространстве, [National Strategy for Trusted Identities in Cyberspace][37].

В основе документа лежит идея единой комплексной многоуровневой безопасной интернет-среды, действующей в условиях достоверной идентификации пользователей, а также надежной защиты их персональных данных. Стратегия ориентирована на физических лиц, а также прочих субъектов (нефизических лиц) — организации, услуги, продукцию программного обеспечения (ПО). Кроме того, стратегия учитывает глобальный характер Сети, подразумевая необходимость действия предлагаемых средств идентификации на трансграничном уровне. Ключевой принцип обеспечения безопасности интернет-среды — позволить всем субъектам коммуникации сообщать свои данные лишь в минимально необходимом объеме в каждом необходимом случае, при многоуровневом и предельно гибком ран-

Евгений ***Сатановский (Россия)****, президент Института Ближнего Востока — по электронной почте из Москвы:* Информационные технологии и кибертехнологии — это всего лишь инструмент революции, равно как и контрреволюции. Электронные СМИ и средства коммуникации позволяют куда эффективнее коллективно организовывать массы, чем газета или кинематограф во времена Ленина. Но и автомат Калашникова лучшее оружие, чем берданка или маузер. Актуальность информационной безопасности и кибербезопасности для традиционного и патриархального в своей основе региона Ближнего Востока — это проблема местных властей, руководства оккупационных сил или лидеров террористических группировок. Все они занимаются этим: одни, чтобы сохранить власть, другие, чтобы ее захватить, третьи, чтобы помешать вторым и поддержать первых. Техническое обеспечение любой войны и революции в ту или иную конкретную эпоху есть прежде всего вопрос о власти. И вопрос архиважный, как говаривал тот же В. И. Ленин с присущим ему грассированием.

жировании требований по тем ли иным транзакциям и разным типам субъектов, в остальных случаях сохраняя анонимность, не сообщая лишнюю информацию.

Для РФ подобные наработки могут представлять весьма большой интерес по следующим причинам:

а) технические средства идентификации в рамках *Экосистемы идентичности* [Identity Ecosystem] максимально диверсифицированы. Это устройства USB, специальное ПО, электронные смарт-карты, компьютерные чипы безопасности, программные сертификаты и даже средства мобильной связи. Весь арсенал технических средств объединяется едиными решениями, а соответствующие программные модули и сертификаты интегрируются едва ли не в любое устройство, позволяющее подключаться к интернету. В этом смысле *Экосистема* следует нынешнему тренду на максимальную диверсификацию средств доступа в интернет и расширение диапазона соответствующих устройств, включая мобильные телефоны;

б) в документе, вопреки опасениям алармистов, четко говорится об отсутствии монопольного контроля над системой со стороны государства и прямо прописан принцип мультистейкхолдеризма. Правительство США планирует строить *Экосистему* на равных началах с бизнесом, НПО и другими субъектами. При этом госорганы должны «показывать пример и быть лидерами в области идентификационных решений»[38]. Такой баланс весьма важен и для России, где традиционное доминирование государства в подобного рода проектах должно находить разумный противовес в лице частного сектора и за счет рассредоточения контроля над системой по мере ее развития;

в) работа в *Экосистеме идентичности* является добровольной для пользователей, которым предоставляется выбор между провайдерами идентификации, способами проведениями транзакций и услугами *Экосистемы*. В данном случае опять же важна диверсификация предлагаемых услуг и решений, которая позволит привлечь пользователей в качестве добровольных клиентов, а не навязывать систему идентификации административными и законодательными методами.

Таким образом, задачей российских органов власти должно стать тщательное изучение данной инициативы, применение ее удачных решений и принципов для разработки аналогичной отечественной концепции целостной системы идентификации пользователей. При этом органичной составляющей подобной системы по умолчанию могла бы стать идентификация пользователей в социальных сетях.

ЗАКЛЮЧЕНИЕ

Суммируя проделанный анализ, целесообразно будет привести ряд выводов и практических рекомендаций.

1. Социальные сетевые сервисы, как и прочие ИКТ, сами по себе не являются источником и причиной социальных волнений, как показали революционные события на Ближнем Востоке. Роль социальных сетей в общественно-политических трансформациях в событиях в арабских странах не была ни монопольной, ни преобладающей среди других средств коммуникации.

Более того, социальные сети не оформились и в качестве негосударственных акторов, подобных ТНК, которые четко осознавали бы свои интересы и возможные стратегии в событиях, подобных *Арабской весне*. Наконец, по тем же причинам лишены оснований утверждения о причастности США к организации и режиссуре *арабских революций*.

В общем и целом социальные сетевые сервисы едва ли представляют угрозу безопасности как на уровне отдельных государств, так и на международном уровне. Соответственно, дискуссия относительно того, как следует реагировать на вызовы безопасности, исходящие от социальных сетей, представляет собой не совсем корректную постановку вопроса. Этот посыл может быть актуален для политического руководства РФ при дальнейшем рассмотрении ими проблематики социальных сетей в плоскости национальной и международной безопасности.

2. Социальные сетевые сервисы могут оказывать деструктивное влияние на международную безопасность в качестве инструментов для проведения того или иного политического курса. Практическим примером такого рода является подход США, в рамках которого указанные сервисы адаптируются с целью подрыва режимов в авторитарных странах, а также для задач шпионажа и военной разведки. Инициативы Соединенных Штатов, направленные на использование социальных сетевых сервисов в таких целях, должны встретить адекватное противодействие международного сообщества, включая РФ. Частью этого процесса должно стать усиление внимания к данной проблематике со стороны ключевых российских ведомств, и в первую очередь МИД, на организационном и структурном уровнях. Верным, но недостаточным шагом в этом направлении является учреждение поста Специального координатора по вопросам политического использования ИКТ в МИД РФ. Процессу расширения соответствующих структурных подразделений МИД должна сопутствовать активизация механизмов межведомственных комиссий. Донесение до международного сообщества российской позиции по использованию социальных сетей в деструктивных целях также является задачей экспертного сообщества, которое должно активизироваться в данном направлении.

3. Одной из приоритетных задач для России в рамках повестки вызовов безопасности в связи с развитием ИКТ должно стать развитие новых проектов в сфере идентификации пользователей, а также анализ зарубежного опыта в этой области.

Необходимо тщательно изучить опыт разработки и ход внедрения проектов комплексного обеспечения безопасности интернета и идентификации пользователей, таких как *Экосистема идентичности*. Данный проект является перспективным примером комплексного подхода к проблеме идентификации. Частично он мог бы стать ориентиром при выработке отечественного системного подхода к идентификации пользователей. Учитывая ограниченность нормативной и концептуальной базы, которой на сегодняшний день располагает в данной сфере Россия,

нам незачем прокладывать свой путь *с нуля*, тратя на это дефицитные ресурсы. Однако, для того чтобы успешно изучить и адаптировать опыт США, российским органам власти необходимо преодолеть нынешний ограниченный подход и скептицизм к американским инициативам в данной сфере. Вместе с тем, разумеется, речь не может идти о механическом копировании американских инициатив — возможным объектом для адаптации здесь выступает сам принцип системных и многоуровневых решений в области идентификации, а отнюдь не конкретные положения концепции *Экосистемы.*

Наработка решений для отечественных проектов подобного рода требует реализации принципов мултистейкхолдеризма с активным и приоритетным участием общественных объединений, бизнеса и горизонтально-вертикальных сетей государственных органов различного уровня. В свою очередь, для осознания актуальности данных принципов российским властям нужен четкий импульс со стороны экспертного сообщества. В число *генераторов* такого импульса мог бы в перспективе войти и ПИР-Центр.

4. Социальные сетевые сервисы могут служить интересам национальной и международной безопасности в областях, не связанных с решением задач международно-политического и военного характера.

На сегодняшний день перспективы имеют как минимум три таких направления:

а) противодействие недружественным информационно-пропагандистским кампаниям;

б) оповещение и информирование населения о чрезвычайных ситуациях и иных угрозах безопасности, сбор и обработка информации о таких угрозах;

в) отслеживание и пресечение противоправной деятельности, включая экстремизм и терроризм.

Выход на устойчивое взаимодействие со структурами интернет-сообщества, которые могут быть полезны в развитии данных направлений, должен стать приоритетной задачей МЧС, МВД, ФСБ, Минобороны РФ и других органов, ответственных за обеспечение безопасности. На данный момент взаимодействие государства с интернет-сообществом развивается, но недостаточными темпами. В числе факторов, препятствующих его развитию, консерватизм и закрытость госструктур в сфере безопасности, отсутствие у них достаточных навыков и мотивации для взаимодействия с интернет-сообществом и гражданским обществом в целом, а также недопонимание технологий социальных сервисов, недооценка их потенциала.

Вместе с тем, по отдельным направлениям, таким как осмысление роли и потенциала ИКТ и глобальных СМИ в контексте деятельности силовых структур, за последнее время достигнут определенный прогресс. Позитивная динамика такого рода должна быть поддержана частным сектором, экспертами и интернет-сообществом и в других областях, связанных с использованием ИКТ и конкретно социальных сетевых сервисов для укрепления национальной безопасности РФ. Определенный вклад в этом направлении, как представляется, может внести и ПИР-Центр.

Примечания

[1] Материал доработан на основе статьи: Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности. *Индекс Безопасности*. 2011, Зима. № 4 (99). С. 59–76.

[2] Boyd, D., Ellison, N. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*. 2007. No 13 (1). http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (последнее посещение — 27 августа 2012 г.).

[3] Policy and Legal Challenges of VirtualWorlds and Social Network Sites — Holger M. Kienle, Andreas Lober, Hausi A. Muller, IEEE Computer Society Washington, DC, USA ©2008.

[4] См. подробнее: The Role of Information Communication Technologies in the «Arab Spring» — Implications beyond the Region. PONARS — Ekaterina Stepanova. Eurasia Policy Memo No. 159. May 2011.

[5] Морозов Е. Цена вопроса. *Газета «Коммерсантъ».* 2011, 9 марта, http://www.kommersant.ru/doc/1595762/print (последнее посещение — 27 августа 2012 г.).

[6] Rachman G. Reflections on the Revolution in Egypt. Financial Times. 2011, February 14, http://www.ft.com/cms/s/0/bc459dfc-3880-11e0-959c-00144feabdc0.html (последнее посещение — 27 августа 2012 г.).

[7] Дмитрий Медведев провел во Владикавказе заседание Национального антитеррористического комитета. Президент России. 2011, 22 февраля, http://kremlin.ru/news/10408 (последнее посещение — 27 августа 2012 г.).

[8] Арабские беспорядки и революции беспокоят Москву. Le Monde, Франция. *ИноСМИ.ру*. 2011, 24 февраля, http://www.inosmi.ru/politic/20110224/166817328.html (последнее посещение — 27 августа 2012 г.).

[9] Корпорация по присвоению имен и номеров в интернете (*англ.* Internet Corporation for Assigned Names and Numbers). Подробнее см. статью в этом номере *Индекса Безопасности*: Якушев М. Интернет–2012 и международная политика. Политические и геополитические аспекты глобального управления интернетом. *Индекс Безопасности*. 2013. Весна. № 1 (104). С. 29–42.

[10] Department of Defense Strategy for Operating in Cyberspace. July 2011. US Department of Defense Official Website. http://www.defense.gov/news/d20110714cyber.pdf (последнее посещение — 27 августа 2012 г.).

[11] Стратегический наступательный твиттер. *Газета.ру.* Александр Артемьев. 2011, 16 февраля, http://www.gazeta.ru/politics/2011/02/16_a_3527294.shtml (последнее посещение — 27 августа 2012 г.).

[12] Следует сразу оговориться в отношении *Wikileaks*. Некоторые эксперты, включая, например, Е.А. Степанову (см. например, исследование The Role of Information Communication Technologies in the «Arab Spring» — Implications Beyond the Region, Ponars — Ekaterina Stepanova. Eurasia Policy Memo No. 159. May 2011) отмечают противоречия в риторике Белого дома о свободе в интернете в свете резко негативной реакции Вашингтона на проект Джулиана Ассанжа. Однако масштабная утечка конфиденциальной переписки дипломатов не смогла ни нанести США действительно серьезный ущерб, ни заставить Белый дом провести ревизию базовых посылов своего курса, оставшись периферийным, хотя и ярким эпизодом в повестке американской политики в отношении киберпространства за последний год. Таким образом, ситуация с *Wikileaks*, хоть и обнаружила наличие двойных стандартов в политике Вашингтона, не привела к отказу Белого дома от борьбы за свободу в интернете во всемирном масштабе.

[13] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Human Rights Council. Seventeenth session. Agenda item 3. General Assembly. 2011. 16 May. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A. HRC.17.27_en.pdf (последнее посещение — 27 августа 2012 г.).

[14] Стратегический наступательный твиттер. *Газета.ру*. 2011, 16 февраля, http://www.gazeta.ru/politics/2011/02/16_a_3527294.shtml (последнее посещение — 27 августа 2012 г.).

[15] Glanz James, Markoff John. U.S. Underwrites Internet Detour Around Censors. *The New York Times.* June 12, 2011. http://www.nytimes.com/2011/06/12/world/12internet.htm?_r=2&scp=2&sq=shadow%20internet&st=cse (последнее посещение — 27 августа 2012 г.).

[16] В северо-западной части КНДР, на границе с Китаем, распространенной практикой среди жителей, желающих передать во внешний мир ту или иную информацию, является передача сообщений и звонков по мобильным телефонам, которые ловят сигнал с китайских вышек, расположенных в холмах через границу.

[17] Белянинов К. Демократию скачают из интернета. *Газета Коммерсантъ.* 2011. 14 июня. № 105/В (4646). http://www.kommersant.ru/doc/1659553?isSearch=True (последнее посещение — 27 августа 2012 г.).

[18] Там же.

[19] Черненко Е. Военные США плетут паутину. *Коммерсантъ*. 2011. 20 июля. № 131 (4672). http://www.kommersant.ru/doc/1682038 (последнее посещение — 27 августа 2012 г.).

[20] Там же.

[21] Алексей Сидоренко. Интервью с автором. 2011.

[22] Там же.

[23] Howe J. The Rise of Crowdsourcing. *Wired.* 2006, June 14, http://www.wired.com/wired/archive/14.06/crowds.html (последнее посещение — 27 августа 2012 г.).

[24] Выступление Государственного секретаря США Хиллари Клинтон по вопросу свободы интернета. Официальный сайт Посольства США в Москве. 2010, 21 января, http://russian.moscow.usembassy.gov/tr_hrc012110.html (последнее посещение — 27 августа 2012 г.).

[25] Встреча с представителями интернет-сообщества. Президент России. 2011, 29 апреля, http://kremlin.ru/news/11115 (последнее посещение — 27 августа 2012 г.).

[26] Генпрокуратура изучит сайты о подпольных казино. *РБК*. 2011, 15 марта, http://top.rbc.ru/society/15/03/2011/559564.shtml (последнее посещение — 27 августа 2012 г.).

[27] Встреча с представителями интернет-сообщества. Президент России. 2011, 29 апреля, http://kremlin.ru/news/11115 (последнее посещение — 27 августа 2012 г.).

[28] Институт современного развития (ИНСОР) создан с целью объединения лучших экспертов для подготовки предложений и выработки документов по важнейшим направлениям государственной политики.

[29] Вражина А. Первая блогерская. Осетинская война в блогосфере. *Lenta.ru.* 2008, 13 августа. http://www.lenta.ru/articles/2008/08/13/blogs/(последнее посещение — 27 августа 2012 г.).

[30] Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве. Информационная безопасность по-русски. *Персональные данные, информационная безопасность и ИТ-инновации*. 2012, 10 февраля, http://www.tsarev.biz/innovation/konceptualnye-vzglyady-na-deyatelnost-vooruzhennyx-sil-rossijskoj-federacii-v-informacionnom-prostranstve/(последнее посещение — 27 августа 2012 г.).

[31] Продвижение в Twitter — вперед, за синей птицей. *Блог ORZ.* 2011, 26 июня, http://blog.orz.com.ua/?p=1251 (последнее посещение — 27 августа 2012 г.).

[32] US Social Network Usage: 2011 Demographic and Behavioral Trends. By Debra Aho Williamson March 2011. 17 Pages, 28 Charts. E-Marketer. emarketer.com/Reports/All/Emarketer_2000777.aspx (последнее посещение — 27 августа 2012 г.).

[33] *ВКонтакте* привлекли к суду из-за песен МакSим. *Lenta.ru*. 2011, 25 апреля, http://lenta.ru/news/2011/04/25/maksim/(последнее посещение — 27 августа 2012 г.).

[34] Чумаченко А. Правильный выбор площадки для продвижения бренда в социальных сетях. *Блог Netpeak*. 2011. 28 апреля. http://netpeak.ua/blog/choose-your-network (последнее посещение — 27 августа 2012 г.).

[35] Банковских карт не оказалось у половины россиян. *Lenta.ru*. 2011. 1 марта. http://www.lenta.ru/news/2011/03/01/cards/(последнее посещение — 27 августа 2012 г.).

[36] *Одноклассники* разрешили «привязывать» к аккаунтам банковские карты. *MoneyNews*. 2011, 6 июля, http://moneynews.ru/News/15271/(последнее посещение — 27 августа 2012 г.).

[37] National Strategy for Trusted Identities in Cyberspace. Creating Options for Enhanced Online Security and Privacy. The White House Official Website. 2010, June 25, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (последнее посещение — 27 августа 2012 г.).

[38] Там же.

Михаил Якушев

МЕЖДУНАРОДНО-ПОЛИТИЧЕСКИЕ ПРОБЛЕМЫ ИДЕНТИФИКАЦИИ В ИНТЕРНЕТЕ

Вопрос об идентификации пользователей глобальной сети, владельцев сетевых ресурсов (как технических, так и информационных), а также лиц, оказывающих те или иные услуги с использованием интернет-технологий, стал одним из наиболее обсуждаемых представителями государственных органов и экспертным сообществом. Так, в Российской Федерации предложения о законодательном «запрете анонимности» в интернете неоднократно высказывались руководителями правоохранительных ведомств в контексте борьбы с преступностью[1]. Указанная проблема также имеет очевидное международно-политическое измерение в силу трансграничного характера сети интернет, особенностей ее архитектуры и развития.

Глобальная сеть стала значимым фактором социально-экономического развития отдельных государств и за последние годы вошла в число важнейших элементов системы международных отношений. Важно понимать, что интенсивность и эффективность использования современных сетевых технологий на национальном уровне сегодня во многом определяют конкурентоспособность той или иной страны на международных рынках. В то же время стабильность и безопасность инфраструктуры интернета требует согласованных действий всего международного сообщества. В этой связи действительно учащаются случаи, когда выявление (идентификация, локализация) пользователей Сети, владельцев размещенной в ней информации, операторов сетевых услуг становится критически необходимым, например, для пресечения использования тех или иных сетевых ресурсов в противоправных целях.

Нельзя не принимать во внимание и общеизвестный факт, что обеспечение юридической возможности идентификации пользователей интернета никогда не являлось ни целью, ни даже характерной чертой построения, функционирования и развития этой сети. Изначально интернет (точнее компьютерная сеть, впоследствии ставшая тем, что мы сейчас воспринимаем как *глобальный интернет*) предназначался для гарантированной и стабильной работы системы управления стратегическими ядерными силами в условиях ведения активных боевых действий. Вследствие этого интернету были и остаются присущи такие особенности, как устойчивость к внешним воздействиям или способность передавать информацию по различным маршрутам в случае выхода из строя значительного числа каналов связи.

Что же касается реального физического местоположения или юридического обозначения отправителей или адресатов электронных сообщений, то эти факторы практически никак не учитывались при разработке технологических принципов построения интернета как информационной сети. Можно сказать, что интернет *технологически нейтрален* по отношению к своим пользователям и при помощи собственных средств (т. е. стандартов и протоколов, описывающих порядок

информационного обмена) не способен определить, кто именно находится за клавиатурой или манипулятором устройства, подключенного к Сети.

Тем не менее вопрос об идентификации участников правовых отношений, связанных с использованием интернета, на практике весьма важен, даже если не принимать во внимание какие-либо политические обстоятельства или соображения публичного порядка. Объем материальных, в том числе финансовых средств, обращающихся в сфере так называемой *интернет-экономики,* исчисляется уже сотнями миллиардов долларов США в год, поэтому достоверная идентификация участников *интернет-экономики* в самом широком смысле этого понятия весьма важна для обеспечения стабильности гражданского оборота, исключения возможностей совершения хозяйственных правонарушений — и этим, вообще говоря, мало чем отличается от необходимости идентификации лиц, участвующих в *традиционных* видах бизнеса. Однако, как известно, даже в *оффлайновом*, то есть обычном бизнесе, не применяющем наиболее современные средства коммуникации, проблема идентификации продавца, покупателя, коммерческого посредника, организатора расчетных отношений и других контрагентов далеко не всегда решается удовлетворительным образом. Особенно в отношениях, как говорят юристы, «осложненных иностранным элементом», когда, например, хотя бы часть из участников сделки находится по разные стороны государственных границ.

Ситуация приобретает еще большую неоднозначность из-за *трансграничности* интернета, при использовании которого затруднительно определить местоположение контрагента, включая лиц, размещающих информацию либо предлагающих иные информационные услуги. Дополнительную сложность вносит отсутствие согласованных на международном уровне норм и правил, которые закрепляли бы допустимую степень анонимности при использовании интернета.

Иначе говоря, при сложившемся разнообразии подходов национальных законодательных систем к регулированию интернета то, что законно в одних странах, будет однозначно запрещено в других. В качестве нейтрального примера достаточно привести азартные игры и порядок идентификации их участников, в том числе в целях недопущения к ним несовершеннолетних. Фактически в настоящее время в интернете существует только одна глобально общепризнанная процедура идентификации — система WHOIS (о которой речь пойдет позже), однако она действует только применительно к администраторам доменов в системе доменных имен DNS.

Таким образом, правомерно попытаться найти ответы на следующие ключевые вопросы, связанные с идентификацией в интернете:

- можно ли создать универсальную, всеобщую, глобально признанную систему идентификации пользователей интернета, операторов интернет-услуг и владельцев сетевых ресурсов?
- если создание такой системы возможно, то на каких принципах и с использованием каких международно-правовых механизмов? Каковы могут быть цели такой идентификации? Как избежать в процессе ее создания и использования нарушений основных прав человека, в том числе права на неприкосновенность частной жизни?
- если создание системы, упомянутой в предыдущем пункте, невозможно, то по каким основным технологическим, организационным, правовым либо иным причинам? Возможно ли в этом случае создание *частных*, ограниченных по территориальному или функциональному признаку систем идентификации?

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Следует учесть, что многие общеупотребительные в повседневном общении понятия могут иметь несколько иные значения в профессиональных дискуссиях,

а также в текстах юридических, в том числе международно-правовых документов. Употребление словосочетания *идентификация в интернете* также может вызвать неоднозначность.

Так, в *философском* смысле понятие *идентификация* означает «установление тождественности неизвестного объекта известному на основании совпадения признаков», что близко по значению к юридическому термину *опознание*. В информационных же системах под идентификацией обычно понимают существенно более *практический* процесс присвоения как субъектам, так и объектам коммуникации определенных *уникальных идентификаторов* и их сравнение с перечнем присвоенных идентификаторов. Например, оконечные устройства телефонных сетей, то есть собственно телефонные аппараты, идентифицируются в процессе установления телефонных соединений по уникальным абонентским телефонным номерам. Но при этом с технологической точки зрения не происходит идентификации лица — гражданина, который участвует в телефонном разговоре, поскольку для этого недостаточно знать, кому указанный телефонный номер был присвоен в соответствующем договоре об оказании услуг связи. Необходимо каким-то образом удостовериться, что именно лицо, указанное в договоре как абонент, в настоящий момент использует данный телефонный аппарат.

Следовательно, для выявления лица, использующего информационные технологии, необходимо говорить не столько об *идентификации*, сколько об *аутентификации* такого лица. Именно аутентификация позволяет установить соответствие названному им идентификатору. Так, в *оффлайновых* отношениях аутентификация производится по фотографии в предъявляемом документе, а иногда по другим биометрическим признакам, включая дактилоскопическую информацию. Кроме того, нельзя смешивать идентификацию и аутентификацию с *авторизацией* — также производимым в информационной системе процессом проверки и подтверждения прав пользователя на выполнение тех или иных действий. Результат авторизации, производимый интернет-технологиями, как правило, без участия человека, зависит от успешной (т. е. достоверной) аутентификации пользователя.

Таким образом, при собственно *идентификации* пользователь интернета «называет себя» информационной системе, подключенной к Сети, например, путем указания своей учетной записи на том или ином информационном ресурсе. При *аутентификации* устанавливается соответствие лица названному им идентификатору. Такая процедура может осуществляться как путем введения пароля или предъявления сертификата электронной подписи, так и иными способами, в том числе биометрическими методами, например, считыванием дактилоскопической информации пользователя. Наконец, при *авторизации* идентифицируемому лицу предоставляются возможности в соответствии с положенными ему правами либо проверяется наличие таких прав.

Все вышесказанное имеет критически важное значение при расследовании случаев неправомерного использования информационных технологий и для привлечения к ответственности виновных в этом лиц. Поскольку задача настоящей статьи более общего плана, допустимо использовать понятие *идентификация* в расширительном плане, понимая под ней любые способы установления идентичности лица, пользующегося сетью интернет либо оказывающего услуги на основе интернет-технологий.

АНОНИМНОСТЬ В ТЕОРИИ И НА ПРАКТИКЕ

Как уже отмечалось выше, одним из аспектов решения вопросов идентификации в интернете является проблема анонимности, пределов допустимости анонимного поведения и определения случаев, когда анонимность должна или может быть законодательно запрещена. Значительная часть правонарушений в интернете осуществляется с использованием анонимных электронных сообщений либо (что точнее) с использованием *псевдонимов* [nicknames], подлинные имена владель-

цев которых не раскрываются, что позволяет по правовым последствиям приравнивать такие случаи к анонимному поведению.

Основной вопрос, который в этой связи требует юридического ответа и, следовательно, согласования соответствующей правовой позиции на международном уровне, сводится к признанию анонимности (*безымянности*) одним из прав человека, а точнее, существенным элементом права на неприкосновенность частной жизни. Что касается правовых режимов использования анонимности, они могут быть сведены к трем основным вариантам:

- анонимность разрешается (допускается) или подразумевается;
- анонимность предписывается;
- анонимность запрещается (не допускается).

Для иллюстрации приведем следующие примеры:

- анонимность разрешается (допускается) в большинстве повседневных, бытовых ситуаций либо когда речь идет о вопросах морального или медицинского плана — например, при анонимном лечении вредных привычек, либо для обеспечения деятельности отдельных видов юридических лиц, таких как акционерные общества[2];
- анонимность напрямую предписывается законом, когда речь идет об избирательной системе, в соответствии с принципом тайны выборов, о защите персональных данных (обезличивание данных социологических опросов и статистических исследований) и, опять-таки, об отдельных случаях, обусловленных морально-этическими и медицинскими соображениями. Примерами последнего варианта служат тайна усыновления, сохранение анонимности доноров при трансплантологии и суррогатное материнство;
- наконец, в ряде случаев анонимность не допускается. Классическим примером является установление личности преступника, совершившего уголовное правонарушение — ведь привлечь к ответственности можно только лицо, которое надлежащим образом идентифицировано и в отношении которого доказана вина в совершении вменяемого ему деяния. Однако запрет на анонимность существует не только в уголовном праве. Практически повсеместно запрещается анонимное владение недвижимым имуществом, а также источниками повышенной опасности. К последним относятся, например, не только оружие, но и транспортные средства, включая автомобили, — у каждого автомобиля есть собственник, идентифицируемый по регистрационному знаку машины.

Кроме того, следует различать анонимность *относительную* и *абсолютную*, а также анонимность *пассивную* и *активную*. Относительной анонимностью можно считать использование средств идентификации таким образом, что реальное имя известно только одному или нескольким контрагентам, но не известно всем остальным. Классические примеры относительной анонимности: публикация анонимного произведения или произведения под псевдонимом в печатном издании, что, собственно, и породило само понятие *аноним*, *безымянное произведение*; сохранение конфиденциальности сведений о банковских счетах, адвокатская, врачебная и иные виды соответствующих тайн; использование телефонной связи с присвоением пользователям уникальных абонентских номеров и т. д. В случае же абсолютной анонимности, по общему правилу, идентификация лица невозможна либо, что бывает намного чаще, не требуется, поскольку при этом ни у кого не возникает каких-либо юридически значимых прав или обязанностей. В повседневной жизни подавляющее большинство ситуаций не предусматривает представления участников общения друг другу, если это не требуется, скажем, общепринятыми нормами вежливого поведения.

Применительно к интернет-технологиям можно говорить о практически абсолютной степени анонимности при подключении к интернету в местах общего доступа (например, в кафе и ресторанах, аэропортах и тому подобных местах), если при этом не требуется авторизации по уникальному паролю, идентифицируемому именно данного пользователя. Впрочем, в ряде зарубежных стран, включая Китай и Белоруссию, при пользовании подобного рода сервисов как раз обязателен если не предварительный ввод уникального идентификатора с паролем, то предоставление уполномоченному сотруднику документа, удостоверяющего личность пользователя. Еще одним примером анонимного использования интернета является участие в дискуссиях онлайн (в комментариях к блогам, новостным сообщениям и т. д.), при которых не требуется идентификация участника дискуссии. Обычно участник дискуссии в этом случае может зарегистрироваться под любым выбранным им псевдонимом, причем указать при регистрации данные о себе, которые не проверяются владельцем интернет-ресурса.

Что же касается понятий *пассивной* и *активной* анонимности, то к первой из них можно отнести все случаи, когда идентифицируемое лицо не называет своего имени, пока его об этом не спрашивают, то есть когда его идентификация не вызывается необходимостью, в том числе не вытекает из каких-либо установленных законодательством предписаний. К *активной* же анонимности относятся ситуации, когда аноним скрывает свое реальное имя даже в случае напрямую обращенного к нему запроса. Наиболее характерным для интернета проявлением анонимности является как раз *пассивная* анонимность.

В большинстве случаев, например, когда пользование Сетью сводится к просмотру интернет-сайтов, идентификации пользователя не требуется. Однако современные интернет-технологии позволяют обеспечивать достаточно высокую степень анонимности и в том случае, когда, с технической точки зрения, пользователь интернет-ресурса *обязан* идентифицировать себя. Так, при обмене сообщениями по электронной почте всегда указывается адрес отправителя, однако при желании отправитель, не желающий быть узнанным, может использовать так называемые *анонимайзеры*, позволяющие создавать временные электронные адреса на любое вымышленное имя и затруднять возможность отследить, через какие почтовые серверы электронное сообщение в реальности прошло, чтобы достигнуть своего адресата. Сходные возможности предоставляют так называемые *прокси-серверы* [proxies][3].

Из вышесказанного легко сделать вывод о том, что *активная* анонимность в *оффлайновом* мире, как, вообще говоря, и стремление добиться некоей стопроцентной абсолютной анонимности, характерны для поведения, скорее характеризуемого как противоправное. В самом деле, для обычного гражданского оборота та или иная степень анонимности допускается, но при необходимости (например, для защиты законных прав третьих лиц) действуют правила раскрытия информации о лицах, выступающих в качестве анонимных, например, в акционерных обществах для этого существуют реестры акционеров. В этих случаях правомерное использование анонимности сочетается с механизмами раскрытия информации в установленных законом случаях. Напротив, при противоправном поведении, например, при совершении уголовно наказуемых проступков, преступник заинтересован в неразглашении информации о себе, чтобы не быть привлеченным к ответственности, то есть стремится к сохранению абсолютной анонимности. В то же время, стремление минимизировать любую возможность идентификации, уничтожение улик характеризует его действия как стремление к активной анонимности.

Подобного рода выводы можно сделать и при анализе вопросов анонимности при использовании интернета. Более того, именно указанные выше факторы и не позволяют поставить знак равенства между понятием *право на анонимность* как одним из компонентов права на неприкосновенность частной жизни и понятием *основные права и свободы человека*[4].

ИДЕНТИФИКАТОРЫ В ИНТЕРНЕТЕ

Несмотря на широкие возможности, которые предоставляют интернет-технологии для использования Сети анонимно или под выбранным самим пользователем псевдонимом, в реальности в интернете существуют самые разнообразные способы идентификации как пользователей тех или иных интернет-ресурсов и их владельцев, так и операторов соответствующих интернет-услуг. По своей архитектуре интернет представляет собой сложную, многоуровневую структуру, на каждом уровне которой мы видим взаимодействие самых различных субъектов, находящихся под различной юрисдикцией.

Так, на самых нижних, так называемых *физическом* и *канальном* уровнях, интернет представляет собой совокупность присоединенных друг к другу и взаимодействующих между собой сетей электросвязи. Каждая из них имеет своего владельца, как правило, оператора связи, имеющего соответствующую лицензию от уполномоченного ведомства страны регистрации данного юридического лица. Сети электросвязи включают каналы связи (оптоволоконные линии связи, спутниковые каналы с наземной и космической инфраструктурой и т. д.), коммутационное серверное оборудование и разнообразные оконечные абонентские устройства. Поскольку все компоненты сетей связи так или иначе являются имущественными объектами, зачастую подлежащими государственной регистрации как недвижимое имущество, идентифицировать владельца того или иного компонента сетевой инфраструктуры не является существенной проблемой.

То же самое можно сказать и об оконечных устройствах, подключаемых к интернету на основании договоров с операторами услуг доступа к Сети. У каждого пользователя такого устройства есть договор с оператором связи с выделением абонентского номера. Например, для пользователей мобильной связи договором выделяется уникальный телефонный номер. В большинстве стран мира, включая Российскую Федерацию, такой договор заключается в письменной форме, с указанием так называемых установочных сведений абонента. В России такими сведениями служат паспортные данные. При необходимости идентификационные сведения из абонентского договора могут быть предоставлены уполномоченным правоохранительным органам в рамках проводимых ими следственно-оперативных мероприятий, а в случае проведения трансграничных расследований в рамках международного сотрудничества, например, по линии Интерпола, в том числе по запросу органов правопорядка зарубежных стран.

На более высоких уровнях архитектурной иерархии Сети, обеспечивающих корректную обработку пересылаемых пакетов информации надлежащим абонентам, применяются идентификаторы подключенных к интернету компьютерных устройств (узлов) в виде набора групп цифр под названием IP-адреса (сетевые адреса)[5]. В настоящий момент используются два вида сетевых адресов, так называемых протоколов 4-й и 6-й версии. При этом второй из них (IPv6) представляет возможность присвоения на несколько порядков большего числа сетевых адресов, чем предыдущий, старый (IPv4). Сетевые адреса распределяются на коммерческой основе пятью региональными сетевыми центрами. Центром, распределяющим адреса для России, является находящаяся в Амстердаме европейская организация RIPE NCC[6]. Получателями сетевых адресов являются уже упомянутые операторы электросвязи, осуществляющие услуги доступа к сети интернет. В принципе, операторы услуг доступа, иногда также именуемые провайдерами [Internet Service Providers], должны в любой момент быть способны определить, кто именно осуществляет ту или иную сетевую активность с использованием установленного сетевого адреса.

Однако на практике, по крайней мере при использовании устаревающего протокола сетевых адресов версии IPv4, затруднения вносит тот факт, что сетевой адрес присваивается не отдельному абоненту, а целой группе пользователей, например, обслуживаемых в рамках одной организации-клиента. Аналогией служит ситуация, когда при оказании услуг телефонной связи организации выделяется один *прямой*

городской номер, а конкретные сотрудники этой организации имеют возможность выхода на телефонную сеть общего пользования через собственный *местный* номер. Разумеется, и в этом случае имеется принципиальная техническая возможность определить, кто именно использовал данный сетевой адрес в конкретный промежуток времени, например, с какого номера телефона был получен доступ в интернет. Однако в отсутствие законодательных требований об обязательном документировании и последующем хранении подобного рода сведений подобного рода достаточно затратные процедуры не всегда выполняются.

Следующим иерархическим уровнем, позволяющим проводить идентификацию интернет-ресурсов и их пользователей, является система доменных имен DNS [Domain Names System]. Система DNS обеспечивает однозначное преобразование сетевых адресов, представляющих набор труднозапоминаемых цифр, в удобное для восприятия сочетание букв, слов или символов, имеющих то или иное значение в национальных языках (например, *pircenter.org* или *правительство.рф*)[7]. Владельцы и администраторы доменов верхнего уровня, таких как *.com, .uk* или *.рф*, заключают специальные соглашения с американской корпорацией ICANN [Internet Corporation for Assigned Names and Numbers], отвечающей за распределение адресного пространства сети интернет. Сведения о том, кто является администратором (так называемой регистратурой) того или иного домена верхнего уровня находятся в открытом доступе в Сети.

Несколько иной подход действует в отношении доменов наиболее востребованного, второго уровня — для идентификации их владельцев применяется сервис WHOIS[8]. Данный сервис отображает довольно подробную информацию о том, на кого и какой организацией-регистратором зарегистрировано данное доменное имя, на каких интернет-серверах размещены использующие этот домен интернет-сайты, а также контактную информацию администратора доменного имени второго уровня и его организации-регистратора. В последнее время в связи с повсеместным принятием законов о защите персональных данных наблюдается тенденция предоставлять минимум сведений о собственно администраторе домена, ограничиваясь ссылками на контактные данные организации, зарегистрировавшей данное доменное имя. Однако в соответствующих зональных регистрах доменных имен должна храниться достоверная информация о каждом владельце доменов второго уровня, которая может быть раскрыта в установленном национальном законодательстве порядке.

В то же время следует признать, что с увеличением числа используемых доменных имен до нескольких сотен миллионов и, соответственно, увеличением организаций-регистраторов доменных имен до нескольких десятков тысяч по всему миру остро встает задача унификации процедур верификации информации, предоставляемой на ресурсах WHOIS. Противоправное использование интернет-ресурсов, например, создание фишинговых сайтов банков в мошеннических целях, при невозможности достоверно определить организатора противоправных действий и владельца созданных в этой связи интернет-ресурсов, идентифицируемых по доменному имени сайта, предельно затрудняет привлечение к ответственности виновных лиц. Данная проблема является основанием для достаточно жесткой критики *бесконтрольности интернета* со стороны заинтересованных политических кругов. Процедуры WHOIS де-факто являются единственным общепризнанным мировым стандартом идентификации владельцев интернет-ресурсов, и в настоящее время ведется дискуссия о необходимости адаптации этих процедур к последним изменениям в системе DNS. В частности, речь идет о совершенствовании процедур WHOIS в связи с появлением доменных имен на нелатинской графической основе, таких как *.рф*[9].

Наконец, отдельной — и едва ли не самой сложной — проблемой является идентификация непосредственно пользователей каждого интернет-ресурса, будь то интерактивный сервис (например, использование социальных сетей) или *пассивный* просмотр интернет-сайта. Уместно начать с того, что даже широко распространенные программные средства просмотра интернет-страниц — веб-

браузеры, не предназначенные по своей сути для идентификации применяющих их пользователей, обеспечивают сбор достаточно подробных сведений о них. Так, при любом посещении интернет-страницы фиксируется следующая информация (причем этот список не является исчерпывающим):

- сетевой адрес (с указанием доменного имени) просматриваемой страницы;
- сетевой адрес страницы перехода, с которой осуществлен переход по ссылке;
- IP-адрес пользователя, из которого определяется наименование провайдера и страна регистрации;
- часовой пояс, в котором находится пользователь;
- данные о применяемых технологиях (таких как cookies, proxy server, Java);
- характеристики интернет-браузера (тип, язык, встроенные расширения, поддержка приложений) и прочие настройки компьютера, включая разрешение экрана и передаваемые цвета.

Очевидно, что вся эта информация, хотя бы по косвенным признакам, в случае надобности может достаточно сузить возможный круг пользователей при проведении соответствующих расследований.

Помимо встроенных программных средств фиксации сведений о пользователе применяются различные способы идентификации непосредственных пользователей отдельных интернет-ресурсов и интернет-сервисов. Приведем примеры наиболее известных их них.

Наиболее часто встречающимся методом аутентификации в интернете является комбинация *«логин (имя учетной записи) + пароль (уникальный набор символов)»*. Однако достоверная информация о пользователе возможна лишь в корпоративных информационных системах, где условные имена пользователей (учетные записи) создаются строго в соответствии с внутрикорпоративными политиками и вероятность получения учетной записи посторонним по отношению к данной корпоративной системе лицом исчезающе мала. В остальных случаях, как правило, пользователь вправе самостоятельно выбрать наименование своей учетной записи и создать собственный пароль — то есть проверка идентифицирующих его документов не осуществляется.

Указанное обстоятельство представляет собой известную *проблему удостоверяющего центра*. Дело в том, что для достоверной идентификации пользователей разных корпоративных систем требуется посредник, третья сторона, которой могли бы доверять все остальные участники взаимодействия и который хранил бы и при необходимости предоставлял данные о владельцах всех учетных записей взаимодействующих информационных систем. Разумеется, реализация в полном объеме требования к удостоверяющему центру может быть достаточно затратной и не удобной для пользователей вследствие громоздкости процедур верификации. Например, такой процедурой может быть личный визит в офис удостоверяющего центра с предъявлением соответствующих документов.

В определенной степени проблема удостоверяющих центров решена в Российской Федерации с принятием в 2011 г. федерального закона «Об электронной подписи»[10], который заменил устаревшие нормативные акты и легитимировал использование в России сразу нескольких видов электронных подписей. Данные подписи предназначены как для подтверждения неизменности электронного подписания после его подписания отправителем, так и для установления личности самого отправителя. Самый защищенный вид электронной подписи, так называемая электронно-цифровая подпись с квалифицированным сертификатом, как раз и предназначен для достоверной идентификации любого пользователя онлайн

сервисов. Однако такая подпись отличается максимальным неудобством в использовании, поскольку процедура ее получения весьма напоминает процедуру заверения у нотариуса собственноручной подписи на бумажном документе. Еще одной проблемой для таких подписей является признание квалифицированных сертификатов за рубежом. Алгоритмы шифрования информации, подтверждающей сведения сертификата, и сам статус российских удостоверяющих центров для зарубежных контрагентов могут и не признаваться надлежащими автоматически, поскольку в мире существует несколько самостоятельных *систем доверия* применительно к электронным подписям.

Более удобны для пользователей, но и более затратны, с материальной точки зрения, аппаратно-программные средства типа электронных карточек доступа, иных средств условного доступа, *электронных паспортов*[11]. Для считывания информации с таких карточек могут потребоваться дополнительные устройства, однако по мере развития технологий способы использования подобных карточек становятся все более удобными. Недостатком указанного метода, помимо относительной дороговизны, является необходимость постоянно иметь карточку условного доступа при себе. Однако, если такая карточка к тому же выполняет функцию обычного удостоверяющего документа типа внутреннего паспорта или водительского удостоверения, данное неудобство скорее становится достоинством. Неоспоримыми преимуществами являются как удобство применения, так и возможность записи на электронную карточку дополнительной информации, позволяющей превратить ее в универсальное средство доступа практически к любому интернет-ресурсу. При этом, что немаловажно, исчезает необходимость запоминания многочисленных паролей и имен учетных записей. Кроме того, такая функция позволяет использовать *электронный паспорт* в трансграничных отношениях, поскольку записанная на нем информация, фактически представляющая собой разновидность электронной подписи, будет соответствовать требованиям максимального числа *систем доверия*.

Также достаточно удобным, а в ряде случаев единственно возможным средством идентификации являются *уникальные цифровые идентификаторы*: номера банковских карточек, номера социального и пенсионного страхования, индивидуальные номера налогоплательщика. Однако следует помнить, что сам по себе ввод такого номера по запросу информационной системы является не средством идентификации, а лишь средством авторизации. Ту же самую идентификационную информацию может ввести лицо, случайным или неправомерным образом получившее доступ к таким идентификаторам, например, получив физический доступ к чужой кредитной карточке. В этом случае указанное лицо будет успешно авторизовано в информационной системе по чужим идентификационным данным.

Отмеченная проблема отсутствует в случае использования так называемых биометрических средств идентификации, Примерами таких средств являются оцифрованная фотография лица, дактилоскопическая карта, эталонная запись голоса пользователя, сканирование радужной оболочки глаза. Степень достоверности идентификации при использовании биометрических средств сегодня намного выше, чем даже пять-семь лет назад, но она все равно не является стопроцентной. Коэффициент ошибок, при которых может быть проведена ошибочная идентификация постороннего человека, либо, наоборот, отказано в авторизации надлежащему пользователю, достаточно велик.

Недостатками биометрических методов идентификации, с одной стороны, является относительная дороговизна необходимой для идентификации аппаратуры. С другой стороны, биометрическую идентификационную информацию почти невозможно изменить, что весьма неудобно по сравнению, например, с паролями. Эта проблема становится особо актуальной в тех случаях, когда идентификационная информация неправомерным образом стала известна третьим лицам и для защиты информационной системы необходимо ее заменить. Кроме того, биометрические сведения во многих странах мира, в том числе в Российской Федерации, рассматриваются как *особая категория* специальных данных. Такие данные

по законодательству подлежат сбору и обработке с определенными ограничениями, обусловленными необходимостью соблюдения прав человека на неприкосновенность частной жизни. Еще более жесткие ограничения чаще всего накладываются на трансграничную передачу биометрических данных. Эти вопросы, как минимум, требуют согласования на уровне дву- или многосторонних межправительственных соглашений.

Развитие интернет-технологий позволило начать использоваться такой способ идентификации, как верифицируемые электронные почтовые адреса. Речь идет об адресах электронной почты, которые принадлежат определенным компаниям (корпоративная электронная почта) или государственным органам и которые предоставляются сотрудникам таких организаций либо лицам, обращающимся за государственными услугами. Как правило, при назначении корпоративного сетевого адреса происходит предварительная верификация пользователя, которому назначается почтовый адрес, а сам такой почтовый адрес содержит фамилию и (или) имя соответствующего пользования. Иначе говоря, маловероятно появление в домене, обозначающего администрацию президента США *.whitehouse.gov*, почтового адреса *barack.obama@whitehouse.gov*, принадлежащего сотруднику по имени Джон Смит. Таким образом, вероятность того, что почтовый адрес вида *(name)@ (corporation domain)* принадлежит именно сотруднику данной организации с указанным в адресе именем, намного выше, чем при использовании любых иных, в том числе бесплатных, почтовых сервисов.

Однако, к сожалению, те же интернет-технологии позволяют имитировать отправку электронного сообщения с иного почтового адреса, что обесценивает возможности верификации отправителя без использования методов, аналогичных средствам электронно-цифровой подписи, или защищенных каналов связи. Впрочем, на корпоративном уровне использование этих средств намного менее обременительно для пользователей и в целом может осуществляться с приемлемым уровнем общих затрат. Проблема остается в признании трансграничных транзакций: необходимо понять, каким способом российский пользователь может убедиться, что домен *.whitehouse.gov* на самом деле имеет отношение к администрации президента США.

Наконец, все более широкое распространение получают способы установления личности пользователей, основанные на иных, специфических видах сетевых идентификаторов. Так, для регистрации учетной записи в некоторых социальных сетях требуется указать номер мобильного телефона, который, в свою очередь, по правилам оказания услуг мобильной связи, может быть предоставлен только абоненту сотового оператора при предъявлении таким абонентом надлежащих идентифицирующих его документов. Может быть и так, что для регистрации в социальной сети и не требуется предоставления какой-либо информации, позволяющей достоверно идентифицировать нового пользования. Однако для последующей активации отдельных сервисов такой сети все же придется указать номер телефона, по которому должно прийти сообщение с кодом активации. Кроме того, для некоторых учетных записей допускается так называемый *верифицированный* или *официальный* статус, для получение которого необходимо предъявить дополнительные документы и/или выполнить ряд дополнительных действий[12].

В свою очередь, учетные записи в социальных сетях и сервисах сами могут служить удобным способом идентификации. Например, название (адрес) пользователя в одной социальной сети может автоматически служить способом авторизации того же пользователя во множестве других, не связанных с такой социальной сетью, сетевых сервисов. Указанные способы идентификации получили название *Open ID* («открытый идентификатор») или «технологии единого входа». Об их популярности может свидетельствовать хотя бы тот факт, что при использовании вебкамер на выборах Президента Российской Федерации для регистрации заинтересованных лиц использовалась именно такая технология[13]. К числу недостатков указанного способа можно отнести разве что возможность несанкционированного доступа сразу ко всем сервисам, в которых зарегистрирован пользователь *пер-*

вичной социальной сети, в случае потери или перехвата его первоначальных идентификационных данных.

Вышесказанное подводит нас к выводу, что применяемые способы идентификации пользователей и владельцев интернет-ресурсов достаточно разнообразны и зависят как от характера собственно сетевого ресурса и политики его владельца, так и от объема прав, предоставляемых пользователю. Безусловно, свою роль играет и трансграничный характер Сети. В частности, для признания надлежащим в одной стране зарубежного идентификатора по технологии единого входа, например, учетной записи в социальной сети *Facebook*, нужна, как минимум, достаточная степень доверия к процедурам идентификации пользователей в данной сети. А в возможной перспективе может потребоваться заключение соответствующего межправительственного соглашения по данному вопросу.

НАЦИОНАЛЬНЫЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ

Наибольшую степень достоверности идентификационных сведений, позволяющую безоговорочно доверять средствам идентификации конкретного пользователя или владельца конкретного интернет-ресурса, могут предоставить различные комбинации применяемых технологий. Однако у всех таких способов есть общий недостаток в виде необходимости привязки существенной части идентифицирующих признаков к программным или организационным средствам, строго регулируемым нормами национального законодательства или не регулируемым вообще, в зависимости от того, о каком государстве идет речь. Так, комбинация *предоставление сведений о себе заявителем + уникальный пароль + указание номера мобильного телефона для последующей авторизации в социальной сети*, вообще говоря, обеспечивает максимальную достоверность при указании телефонного номера *только* в той стране, где возможен доступ к установочной информации о владельце такого номера.

Различные способы подразумеваемой идентификации (например, признание пользователя *другом* иными пользователями социальной сети), дополнительный верифицируемый статус учетных записей, использование технологий единого входа и другие моменты ставят вопрос о надежности оператора социальной сети как посредника в идентификации ее пользователей. Проблема становится особо актуальной, когда владелец такой сети находится под юрисдикцией одного государства, а вопросы об идентификации его клиентов возникают в другом. Еще один способ идентификации, при котором в дополнение к предоставляемым сведениям требуется предоставить сканированные копии подтверждающих их бумажных документов, с одной стороны, не исключает возможности фальсификаций, а с другой — наталкивается на сложности трансграничной передачи указанных персональных данных.

Наконец, применяемый в России способ идентификации пользователей Портала государственных услуг[14], при котором пароль доступа высылался по указанному заявителем адресу обычной, не электронной почтой (на что могли уходить несколько дней или даже недель), вряд ли сможет когда-либо получить международное признание в онлайновых транзакциях. Впрочем, то же можно сказать и об эстонских ID-картах, поскольку записанная на них информация в полном объеме может быть считана и достоверна оценена только на территории Эстонской Республики.

Таким образом, встает задача не только создания общенациональных систем идентификации пользователей и владельцев интернет-ресурсов, но и сопряжения таких систем между собой для обеспечения среды доверия, среды достоверного обмена идентификационной информацией в интернете.

В России указанная проблема находится на начальном этапе ее решения. Задачи общенациональной идентификации в интернете не сформулированы, если не считать отдельных заявлений руководителей правоохранительных органов. Также

отсутствует законодательное регулирование данного вопроса. К примеру, порядок использования Портала государственных услуг или вебкамер в избирательном процессе был установлен распорядительными, а не нормативно-правовыми актами. По сути, единственным формально регламентированным, но применяемым относительно редко способом идентификации в РФ является технология электронной подписи.

Более системно указанные задачи решаются в Китайской Народной Республике[15]. Так, операторы доступа к сети интернет обязаны иметь лицензию Министерства промышленности и информатизации Китая, при этом доступ к точкам трансграничного обмена трафиком имеют лишь девять таких операторов. Все интернет-пользователи на территории КНР подлежат идентификации по паспорту или заменяющему его документу при заключении договора об оказании услуг доступа к интернету, при этом каждому пользователю предоставляется уникальный идентификатор. Администраторами доменных имен могут быть только юридические лица, имеющие лицензию на право торговой деятельности на территории КНР, или зарегистрированные средства массовой информации.

Наконец, операторами контент-услуг (т. е. распространителями информации) на территории Китая могут быть только лица, являющиеся администраторами доменных имен либо имеющие договоры с операторами доступа. При этом распространение информации возможно только при наличии договора с правообладателями. Разумеется, при такой подробной регламентации на каждом этапе получения (предоставления) интернет-услуг проводится надлежащая идентификация пользователей и операторов сетевых ресурсов. Однако при этом не предоставляется открытого доступа онлайн к информации о реестре операторов или пользователей, вследствие чего китайская система интернет-идентификации *автоматически* не может быть полезной для зарубежных правоохранительных органов. Для проведения межправительственных процедур взаимодействия таких органов требуется оформление письменных запросов.

Противоположная картина складывалась до недавнего времени в Соединенных Штатах, где формально отсутствовали какие-либо нормативные требования к системе идентификации в интернете. В этой связи представляет особый интерес инициатива президента США Барака Обамы в области Национальной стратегии доверительной идентификации в киберпространстве от 2011 г. [National Strategy for Trusted Identities in Cyberspace][16]. В документе ставится задача повышения надежности идентификационных данных и степени защиты информации, которая позволяет установить реальную личность пользователя. Вследствие разнообразия видов и большого числа учетных записей (паролей, других средств авторизации) предложено создание трехуровневой *Экосистемы идентичности* [Identity Ecosystem][17].

При этом предлагается добровольный принцип участия в *Экосистеме идентичности* и допускается как возможность информационного обмена без полной идентификации его участников, так и использование самых различных сетевых средств идентификации и корреляция их с данными, накапливаемых вне сети (в оффлайне). Сама по себе Национальная стратегия подробно не рассматривает вопросов сопряжения американской *Экосистемы идентичности* с зарубежными аналогами, предполагая, что именно американские предложения станут де-факто стандартом на международном уровне.

Вопросы идентификации в интернете частично затрагиваются и в российском проекте концепции Конвенции об обеспечении международной информационной безопасности (2011 г.)[18]. В качестве дополнительных факторов, усиливающих опасность угроз информационной безопасности, в документе указывается «неопределенность в идентификации источника враждебных действий, особенно с учетом возрастающей активности отдельных лиц, групп и организаций». Также в этом списке фигурируют «различия в национальных законодательствах».

Концепция Конвенции предлагает государствам-участникам «стремиться к гармонизации национальных законодательств, при этом различия в них не должны создавать барьеры на пути формирования надежной и безопасной информационной среды». Также фиксируется принцип ответственности каждого государства-участника «за собственное информационное пространство, в том числе и за его безопасность и содержание размещаемой в нем информации». В частности, в целях организации уголовного процесса государства-участники должны принимать «законодательные и иные меры, необходимые для того, чтобы гарантировать оперативное предоставление компетентным органам государства-участника или лицу, назначенному этими органами, достаточного количества данных о потоках информации, которые позволят идентифицировать поставщиков услуг и путь, которым передавалось конкретное сообщение в информационном пространстве».

Исходя из практики создания и функционирования национальных систем идентификации и решений, предлагаемых на международном уровне, можно говорить о складывающемся консенсусе по поводу того, в каких случаях в интернете не должна предоставляться бесконтрольная анонимность и, напротив, должна проводиться идентификация пользователей, операторов, владельцев ресурсов (источников информации и соответствующих угроз):

- совершение противоправных действий (мошенничества, кражи идентичности и других преступлений);
- распространение незаконной информации (антиобщественного характера, не предназначенной для детской аудитории и т. п.) либо вредоносных программных средств;
- террористические угрозы (воздействие на общественное мнение, создание паники, распространение слухов и другие действия террористической направленности);
- незаконное получение информации, представляющей объекты интеллектуальной собственности;
- необходимость прекращения прав третьих лиц. Подразумевается, что защищать необходимо не только права анонимных пользователей, но и в равной степени законные права любых третьих лиц.

Разумеется, при этом требуется соблюдать принцип соразмерности ограничения прав, гарантированных основными, в том числе международными, правовыми актами. Кроме того, при любых обстоятельствах пользователь интернета имеет право знать и должен быть уведомлен о том, какие права он имеет, какие обязательства при использовании сетевых ресурсов несет и какие ограничения и при каких обстоятельствах могут у него возникнуть. Вся информация подобного рода, как правило, описывается в соответствующих пользовательских соглашениях каждого интернет-ресурса.

ВЫВОДЫ И РЕКОМЕНДАЦИИ

1. Простых и быстрых решений проблем, возникающих в связи с необходимостью идентификации в интернете, на данный момент не просматривается ни на национальном, ни, тем более, на международном уровне.
2. В силу разнообразия используемых в разных странах и в различных ситуациях мер идентификации, аутентификации и авторизации любые решения, принимаемые на локальном или национальном уровне, могут быть эффективны *только* на территории данной страны. Попытки распространить такие решения на иные сферы применения чреваты конфликтами, в том числе на межгосударственном уровне. Кроме того, такие решения могут быть в принципе неэффективными, а нарушение принципа технологической нейтральности интернета способно привести к реальной

сегментации Сети и отразиться на стабильности ее развития в соответствующих сегментах.

3. Введение каких-либо общеобязательных мер всеобщей идентификации, например, по образцу Китая, может быть оправдано только при заранее обозначенной цели, соразмерной объему и обременительности предлагаемых мер. Без комплексного подхода, в том числе в отношении ограничения доступа к информации, признаваемой антиобщественной, такие меры будут либо бесполезны, либо легко обходимы.

4. Право на анонимность является составным элементом законного права на неприкосновенность частной жизни и в этом качестве должно безусловно признаваться и уважаться. Однако абсолютное право на анонимность невозможно. Можно лишь говорить о допустимой степени относительности такого права, поскольку *абсолютная анонимность = абсолютный криминал*. Следовательно, ограничения права на анонимность должны быть соразмерны, установлены национальным законом и соответствовать общепризнанным принципам международного права.

5. Не могут и не должны ограничиваться в *онлайне* права и свободы, гарантированные для *оффлайна*. Следовательно, случаи и порядок идентификации пользователей, операторов и владельцев сетевых ресурсов не должны в правовом смысле отличаться от случаев и порядка идентификации лиц, не использующих интернет. В противном случае пользователи и операторы интернета будут явным образом дискриминированы.

6. Российским органам власти следовало бы отказаться от идеи введения обязательной идентификации в интернете, что бы под такой идентификацией ни подразумевалось. Необходимо определить цели *реально необходимой* идентификации и сфер применения, в которых подобная идентификация целесообразна. Необходим и диалог между заинтересованными органами власти, организациями интернет-бизнеса, экспертным сообществом и представителями гражданского общества по техническим и правовым мерам, отвечающим заявленным государством целям идентификации.

7. Используя опыт работы в интернете российских и зарубежных компаний, признать возможным использование различных способов и методов идентификации и начать работу по легализации в России технологий единого входа, подобных Open ID. При необходимости возможно подключение к этой технологии государственных и муниципальных органов. Правоохранительным органам, причем не только российским, следует уделить особое внимание тактике и методике использования систем авторизации во взаимодействии с операторами соответствующих сетевых сервисов.

8. Российские государственные органы совместно с компаниями IT-сектора могли бы провести комплексные НИОКР по внедрению в нашей стране зарекомендовавших себя и перспективных способов идентификации, которые доказали высокую эффективность в отдельных, критически важных сферах применения. К числу подобных мер можно отнести распространение среди населения программно-аппаратных средств электронной подписи, развитие технологий единого входа, развитие биометрических средств идентификации, создание верифицируемых средств создания электронных почтовых адресов и использования защищенных каналов обмена электронными документами с этих адресов без предоставления и использования средств электронной подписи пользователями.

9. В повестку дня международных форумов с участием Российской Федерации должны быть внесены вопросы создания *Международной экосисте-*

мы идентификации в интернете. Такая экосистема должна обеспечивать взаимное признание различных видов идентификаторов (пользователей интернета, операторов интернет-услуг, владельцев интернет-ресурсов) независимо от их местонахождения. Для этого, в частности, требуется заинтересованное изучение американской Национальной стратегии по доверительной идентификации в интернете в целях допустимости ее положений на практике в российских и иных реалиях использования интернета. Рассмотрение такого практического для всех стран мира вопроса, как идентификация в интернете, особенно в деполитизированном и *неконфронтационном* формате, способно благоприятно воздействовать на обеспечение международного мира и безопасности применительно к развитию интернета.

Примечания

[1] Полицейское управление «К» предложило запретить анонимные выступления в интернете. *Российская газета: Федеральный выпуск.* 2011, 8 декабря. № 5652 (276), http://www.rg.ru/2011/12/08/moshkov.html (последнее посещение — 31 августа 2012 г.).

[2] В ряде европейских языков акционерные общества как раз и называются анонимными, поскольку для их деятельности не требуется раскрытие имени акционеров. Так, по-французски акционерное общество звучит как *societ'e anonyme*.

[3] Подробнее см., например: Часто задаваемые вопросы о proxy (proxy FAQ). *CIT Forum*. http://citforum.ru/internet/webservers/proxy_faq (последнее посещение — 31 августа 2012 г.).

[4] О *праве на анонимность* см. подробнее:

The right to anonymity on Internet and legal implications. *Security Affairs.* 2012, June 14, http://securityaffairs.co/wordpress/6452/intelligence/the-right-to-anonymity-on-internet-and-legal-implications.html (последнее посещение — 31 августа 2012 г.).

Gapper G. It is right to curtail web anonymity. *Financial Times.* 2011, August 31, http://www.ft.com/cms/s/0/f3637672-d31e-11e0-9ba8-00144feab49a.html#axzz259kp6VPc (последнее посещение — 31 августа 2012 г.).

Якушев М. Анонимность в интернете и право на неприкосновенность частной жизни. Координационный центр Национального домена сети интернет, http://cctld.ru/files/ppt.pptx (последнее посещение — 31 августа 2012 г.).

[5] Более подробно см. статью в этом номере *Индекса Безопасности*: Якушев М. Интернет-2012 и международная политика. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 36.

[6] RIPE NCC. RIPE Network Coordination Centre, http://www.ripe.net (последнее посещение — 31 августа 2012 г.).

[7] Более подробно см. статью в этом номере *Индекса Безопасности*: Якушев М. Интернет-2012 и международная политика. С. 36–38.

[8] От английского WHO IS (it) дословно КТО (есть) ЭТО.

[9] Подробнее см.: WHOIS Policy Review Team Draft Report. Internet Corporation for Assigned Names and Numbers. 2012, March 18, http://www.icann.org/en/news/public-comment/whois-rt-draft-final-report-05dec11-en.htm (последнее посещение — 31 августа 2012 г.).

[10] Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ (принят Государственной Думой Федерального собрания Российской Федерации 25.03.2011).

[11] Например, ID-карты, широко применяющиеся в Эстонии.

Подробнее см., например: Цифровое подписывание. ID. Удостоверение личности нового поколения. 2012, 10 мая, http://www.id.ee/?id=11080&&langchange=1 (последнее посещение — 31 августа 2012 г.).

[12] См., например: Страница председателя правительства Российской Федерации Дмитрия Анатольевича Медведева. Facebook, http://www.facebook.com/Dmitry.Medvedev (последнее посещение — 31 августа 2012 г.).

[13] Доступ к архиву видеотрансляции выборов Президента Российской Федерации. Электронное правительство. Госуслуги,

http://epgu.gosuslugi.ru/pgu/service/-10000000413_418.html#_description (последнее посещение — 31 августа 2012 г.).

[14] Электронное правительство. Госуслуги, http://epgu.gosuslugi.ru (последнее посещение — 31 августа 2012 г.).

[15] Более подробно см., например: Цензура Интернета в Китае. Ваш личный Интернет. 2005, 16 июня, http://www.content-filtering.ru/allinet/regulinet/regulinet_249.html (последнее посещение — 31 августа 2012 г.).

Также см. статью в этом номере *Индекса Безопасности*: Ибрагимова Г. Стратегия КНР в области управления интернетом и обеспечения информационной безопасности. С. 169–184.

[16] National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy. 2011. May,

http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (последнее посещение — 31 августа 2012 г.).

[17] Более подробно об *Экосистеме идентичности* см. статью в этом номере *Индекса Безопасности*: Демидов О. Социальные сетевые сервисы в контексте национальной и международно безопасности. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 81–83.

[18] Более подробно о концепции Конвенции см. статью в этом номере *Индекса Безопасности*: Демидов О. Международное регулирование информационной безопасности и национальные интересы России. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 99.

Галия Ибрагимова

ПОДХОДЫ ГОСУДАРСТВ ЦЕНТРАЛЬНОЙ АЗИИ К ВОПРОСАМ УПРАВЛЕНИЯ ИНТЕРНЕТОМ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Интернет — технология, объединившая компьютерные сети для передачи данных, — вряд ли приобрел бы свое сегодняшнее значение и основополагающую роль в современной системе информационного обмена, если бы не пользователи, наполнившие его контентом. Ожившая *псевдореальность,* созданная интернет-пользователями, уничтожила понятие границ и создала возможности для глобальной коммуникации. Свобода слова, ранее казавшаяся иллюзорной и не досягаемой для жителей множества стран, вдруг стала реальностью, обрушилась на цензоров, и в то же время подстегнула процессы, подчас угрожающие дестабилизацией сложившегося социально-политического строя в различных странах и регионах мира. *Оранжевые революции* на постсоветском пространстве, революционные события на Ближнем Востоке — все эти события стали убедительным свидетельством мощи и влияния интернет-коммуникаций на процессы, происходящие в современном мире. Виртуальная реальность вторглась в казавшиеся устойчивыми и незыблемыми социально-политические процессы и начала трансформировать современный миропорядок.

Центральная Азия[1], где еще несколько лет назад проблема информационного неравенства была одной из наиболее острых, сегодня активно осваивает современные информационно-коммуникационные технологии (ИКТ). Интернет в республиках региона — пока еще не обыденность для большинства граждан, но в то же время он уже перестал быть экзотикой. На начало 2012 г. доступ к глобальной сети имели около 16,1 млн жителей центральноазиатских государств[2]. Любопытно, что в Узбекистане, который неоднократно подвергался критике и обвинениям в ограничении доступа к интернету, число интернет-пользователей (7,55 млн человек) существенно превышает аналогичный показатель других государств региона[3]. Это означает, что доступ в сеть пользователей, освоивших интернет-навигацию хотя бы на среднем уровне, довольно сложно эффективно блокировать. Более того, попытки заблокировать массовую интернет-аудиторию от доступа в интернет по большей части бессмысленны и неосуществимы, по крайней мере, в отсутствие сложных системных решений наподобие *Великого китайского файрвола.*

Доказательством мощного потенциала влияния сетевых технологий на социальные и политические процессы в регионе служит пример трагических событий на юге Киргизии в 2010 г. Тогда информация о происходящих событиях в основном распространялась посредством социальных сетей на фоне преимущественного молчания государственных СМИ. Пользователи соцсетей организовывались в патрули добровольцев для защиты Оша и Бишкека от грабежей и мародерства. Через интернет была организована гуманитарная помощь для беженцев и пострадавших во время этнических столкновений. При этом в сборе гуманитарной помощи приняли участие не только жители Киргизии, но и Узбекистана, Казахстана,

Таджикистана, которые были мобилизованы через социальные сети *Facebook, ВКонтакте, Одноклассники, Мой Мир*. Данные события стали свидетельством того, что в государствах Центральной Азии интернет, несмотря на скромные показатели проникновения, в целом развивается в соответствии с общемировыми тенденциями в сфере ИКТ.

Несомненно, развитие интернет-инфраструктуры в Центральной Азии на сегодняшний день сталкивается с определенными трудностями. Имеют место попытки заблокировать доступ к веб-сайтам оппозиционных партий и СМИ, распространяющих в сети критическую информацию о власти, практикуются DDoS-атаки сайтов, содержащих порочащий деятельность госструктур контент, фильтруются новости о событиях в регионе, отслеживается активность участников социальных сетей и блогеров, идут ожесточенные *войны интернет-троллей*[4]. Эти действия обусловлены специфической политикой в области информационной безопасности, проводимой центральноазиатскими властями для защиты национальных интересов.

Каждая центральноазиатская республика формирует собственные подходы к обеспечению информационной безопасности, которые находят отражение в национальных законодательствах. Практически во всех государствах региона есть специальные комиссии по проблемам информационной безопасности, принимаются межправительственные соглашения по защите информационного пространства. Однако следует признать, что проблема до сих пор теоретически не проработана.

Чаще всего под информационной безопасностью в государствах региона понимается защита национального информационного пространства от негативного и деструктивного информационного воздействия внешних сил. При этом за негативное внешнее влияние власти часто принимают любую информацию, содержащую критику в адрес правительства и других структур власти. В законодательствах стран Центральной Азии зачастую отсутствуют четкие формулировки понятия *информационная безопасность*. Недостаточное внимание уделяется вопросу управления интернетом. Подобный подход увеличивает уязвимость региона перед внешними информационными вызовами и угрозами. Даже в отсутствие предварительного анализа актуальна задача развития республиками региона собственных сегментов информационного пространства и выработки ими единого для Центральной Азии подхода к обеспечению информационной безопасности. Движение в этом направлении, как представляется, стало бы существенным вкладом не только в развитие информационного пространства, но и в национальную безопасность региона.

Задача настоящей статьи — проведение краткого сравнительного анализа подходов стран Центральной Азии к обеспечению информационной безопасности, а также к вопросам управления интернетом.

ТАДЖИКИСТАН

Таджикистан стал первым государством Центральной Азии, принявшим национальную Концепцию информационной безопасности — еще в 2003 г. такой документ был разработан и утвержден правительством страны. В концепции подчеркивается роль информации для развития республики, а информационная сфера обозначена как системообразующий фактор жизни общества. Документ активно используется для определения многих терминов и механизмов обеспечения безопасности в информационной сфере, его положения используют органы государственной власти для формирования и проведения политики информационной безопасности.

Под информационной безопасностью Республики Таджикистан понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства[5]. Ведущую роль в обеспечении информационной безопасности Таджикистана играет государство, которое ответственно за качественное форми-

рование и развитие информационной инфраструктуры исходя из общенациональных интересов. Примечательной особенностью концепции является то, что в ней классифицированы стратегические задачи внутренней и внешней политики государства по обеспечению информационной безопасности. Основные принципы обеспечения информационной безопасности авторы документа видят в соблюдении конституционных прав человека на получение информации, информационном обеспечении государственной политики, доведении до населения и международной общественности достоверной информации о государственной политике.

На фоне этих *правильных* постулатов концепция признает и наличие в Таджикистане ряда проблем, в первую очередь социально-экономического характера, которые препятствуют полноценному развитию информационно-коммуникационных технологий в стране. Примечательно, что решение проблемы информационного неравенства в Таджикистане связано с увеличением *импорта ИКТ*, в то время как соседи по региону, наоборот, рассматривают снижение зависимости от зарубежных информационных технологий и развитие собственного производства в этой области в качестве одного из главных механизмов обеспечения национальной информационной безопасности. Особое внимание в Концепции уделяется развитию отечественной индустрии информации, в том числе СМИ, которые призваны обеспечивать идеологическую защиту государства, общества и личности от современных информационных вызовов и угроз[6]. В документе также выделяются информационные угрозы, которые могут представлять опасность для внешней политики страны. Перечень их включает дезинформацию, пропаганду, ведение информационных войн, информационное воздействие иностранных политических, экономических, военных и информационных структур на реализацию стратегии внешней политики Республики Таджикистан.

В документе также выделяется *набор* правовых, организационно-технических, экономических, политических методов обеспечения информационной безопасности. Правовое обеспечение информационной безопасности осуществляется согласно существующей нормативо-правовой базе, которая на сегодняшний день включает довольно несистемный перечень нормативно-правовых актов[7].

Обеспечение безопасного функционирования интернета также является приоритетным направлением таджикской политики информационной безопасности. Интернет в Таджикистане начал развиваться с 2001 г., когда на базе акционерного общества *Таджиктелеком* была создана общая республиканская сеть с последующим подключением к ней корпоративной сети. Тогда же было принято постановление правительства Республики Таджикистан «О создании республиканской сети передачи данных и мерах по упорядочиванию доступа к мировым информационным сетям». Этот документ был одним из первых, который на законодательном уровне регулировал все процессы в области интернет-технологий. В 2011 г. количество интернет-пользователей составило 600 тыс. человек, число таджикских интернет-сайтов превысило 600. Эти показатели намного меньше аналогичных в соседних республиках региона. Для республики по-прежнему характерна проблема информационного неравенства — доступ к интернету вообще не имеют более 70% населения страны. Вместе с тем нынешние темпы роста таджикского сегмента интернета позволяют предположить, что в ближайшее время в Таджикистане будет все же сформирован полноценный таджикский интернет-сектор, который охватит бо́льшую часть населения.

Одна из особенностей информационного пространства республики состоит в том, что государство, несмотря на доминирующее положение, проявляет готовность способствовать росту числа независимых частных СМИ и сотрудничать с ними на равноправной основе. Особый приоритет отдается электронным масс-медиа, в том числе размещенным в интернете. Таджикистан привлекает крупных, в том числе иностранных, инвесторов для финансирования различных информационных проектов. Примером участия иностранного капитала в СМИ Таджикистана является деятельность информационного агентства (ИА) *Азия-Плюс*. Ежедневно интернет-сайт информационного агентства посещают более семи тысяч пользователей.

Ресурс предусматривает предоставление собственной информации в режиме онлайн, выставляются также электронные версии или отдельные статьи из газеты *Азия-Плюс*, журнала *VIP-zone*, каталог фоторепортажей, видеосюжетов, блоги и масса различной справочной информации. Не менее популярным новостным интернет-ресурсом является сайт *Азия-Плюс*, входящий в медиахолдинг *Авеста*. Посещаемость этого сайта составляет три тысячи человек в день. Популярность этих ресурсов обусловлена тем, что контент размещается одновременно на русском, английском и таджикском языках. Большинство других зарегистрированные в Таджикистане интернет-СМИ существенно уступают вышеназванным ресурсам как по количеству, так и по качеству предоставляемых услуг[8].

Широкое участие бизнес-структур в индустрии электронных масс-медиа ведет к тому, что они становятся значимыми участниками медиа-рынка и начинают составлять конкуренцию государству. Государство, в свою очередь, проявляет готовность воспринимать некоторые частные СМИ как *равноправных партнеров*. Во многом это опять же обусловлено событиями *Арабской весны*, которые показали, что новые медиа не только превращаются в важный фактор внутренней общественно-политической дискуссии, но и становятся одним из наиболее существенных инструментов позиционирования страны и формирования ее имиджа на международной арене. Можно сказать, что СМИ Таджикистана находятся на пути трансформации из инструмента политики и идеологии правящей партии в относительно независимый и влиятельный общественный институт.

Социальные сети и блоги также пользуются большой популярностью в Таджикистане. Но таджикистанцы используют социальные сети не только как средство для общения и развлечения, но и для свободного выражений своих взглядов на проблемы внутриполитического развития республики. *Facebook*, где зарегистрировано 26 тыс. пользователей, до марта 2012 г. являлся единственной площадкой в стране, где можно было свободно обсуждать самые острые проблемы и критиковать власть[9]. Но критикой власти таджикские пользователи не ограничились. При помощи *Facebook* в стране были организованы десятки различных акций. Наиболее заметной стала акция, проведенная весной 2011 г. Весна — это наиболее сложный период для жителей Таджикистана, так как в это время доступ к электроэнергии жестко лимитируется. Так, группа молодых активистов собралась у здания *Барки точик* — государственной энергокомпании, основного поставщика электричества в стране — и устроила символические *похороны энергетики*. Организаторы *флэшмоба* рассчитывали на жесткую реакцию властей, однако все прошло относительно спокойно. Активное освещение акции местными СМИ стало своеобразной рекламой возможностей современных интернет-ресурсов для массовой коммуникации. Таджикские интернет-пользователи осознали, что *Facebook* можно и в местных условиях использовать в качестве действенного инструмента мобилизации общественных масс с целью артикуляции и решения острых социально-экономических проблем как локального, так национального масштаба.

Через социальные сети в Таджикистане также были организованы десятки благотворительных акций: помощь детям-сиротам, домам престарелых, инвалидам, общественных уборок территорий от мусора, культурные мероприятия. Таджикские пользователи *Facebook* неоднократно обращались к правительству страны и президенту с призывами решить наиболее острые проблемы общества. Для этого в социальной сети было создано специальное *комьюнити Платформа,* где участники могут обратиться к власти и высказать свое мнение по поводу процессов, происходящих в общественно-политической и экономической жизни республики, поделиться волнующими их проблемами. Но попытки активистов группы привлечь к обсуждению властные структуры не увенчались успехом. Чиновники избегают вступать в дискуссии с участниками соцсетей и блогерами. К тому же события *Арабской весны*, создавшие убедительную видимость того, что при помощи социальных сетей, мобильной коммуникации и блоговых сервисов возможно мобилизовать население для свержения правящих режимов, насторожили власти Таджикистана. 5 марта 2012 г. в соответствии с указанием Государственной комис-

сии по телекоммуникациям на территории республики был заблокирован доступ к *Facebook*. Помимо популярной соцсети был заблокирован доступ к сайтам *TjkNews.com* и *Zvezda.ru,* — по всей видимости, за критику в адрес действующей власти[10]. Еще одним распространенным поводом для блокирования веб-сайтов в Таджикистане является угроза распространения материалов экстремистского характера, в частности информации, распространяемой *Исламской партией Таджикистана*. Однако, несмотря на практикуемые государственными органами интернет-цензуру и блокировку сайтов, таджикские пользователи всемирной сети находят способы обходить все препоны и при помощи таких нехитрых средств, как *прокси-серверы,* свободно пользоваться интернет-ресурсами.

Вместе с тем в Таджикистане имеет место тенденция к созданию собственных социальных сетей в доменной зоне .tj. Одним из наиболее масштабных проектов в этой сфере стало создание социальной сети *mymlt.tj*. Однако возможности наполнения и концепция соцсети в основном ограничиваются развлекательной тематикой. Еще одной популярной в республике интернет-площадкой для общения таджикистанцев является сайт *from.tj*. На сайте существует форум, где можно создать тему и привлечь к ее обсуждению зарегистрированных на сайте пользователей. Также на сайте можно завести блог и публиковать записи на различные темы. Среди наиболее обсуждаемых тем — вопросы социального развития Таджикистана, культурные мероприятия в стране, национальная история.

КАЗАХСТАН

В Республике Казахстан основные направления обеспечения информационной безопасности до последнего времени были закреплены в Концепции информационной безопасности от 2006 г.[11]. Документ предлагал довольно общую типологизацию угроз информационной безопасности республики, подразделяя их в зависимости от происхождения на внешние и внутренние, технические и идеологические. Стратегическими задачами концепции назывались формирование единого информационного пространства Казахстана и создание условий для его качественного развития.

Следует подчеркнуть, что и до принятия данной концепции вопросы информационной безопасности находили отражение в целом ряде законов и иных нормативно-правовых актов республики[12]. Но обилие нормативно-правовых документов, не сведенных до принятия Концепции в единую систему, вело к довольно хаотичному состоянию сферы информационной безопасности и отсутствию единой четкой доктрины. Положения законов в ряде случаев противоречили друг другу, что обусловливало дублирование функций и вносило дезорганизацию в деятельность субъектов, призванных обеспечивать безопасность информационного пространства страны. Таким образом, толчком для создания единой национальной Концепции стало стремление упорядочить законодательную базу в сфере информационно-коммуникационных технологий и повысить ответственность субъектов, действующих в сфере информатизации.

Одна из особенностей Концепции от 2006 г. заключалась в том, что в ней впервые в практике СНГ введено понятие *управление интернетом*, под которым понимались разработка и применение правительством, частным сектором и всем гражданским обществом общих принципов, правил, процедур принятия решений, регулирующих использование интернета[13]. В то же время в числе недостатков первого в Казахстане *доктринального документа* по вопросам информационной безопасности было отсутствие четкого понятийного аппарата — например, в Концепции не определялось само понятие *информационной безопасности.*

Следующим этапом развития казахстанского законодательства в этой области стала Концепция информационной безопасности до 2016 г., утвержденная Указом президента республики от 30 сентября 2011 г. Новый документ стал существенным шагом вперед сразу по нескольким направлениям. Во-первых, концепция

аккумулировала и отразила в себе международный опыт в части обеспечения информационной безопасности[14]. Так, среди государств, чьи наработки изучались и использовались при выработке нового казахского видения безопасности в области ИКТ, указываются США, Великобритания, Канада, Российская Федерации, Индия, Эстония. Опыт изучения документов государств с высокоразвитым и диверсифицированным ИТ-сектором косвенно свидетельствует об изменениях и развитии информационного сектора в самом Казахстане. Кроме того, в концепции отражен и частично инкорпорирован багаж международного сотрудничества страны в области информационной безопасности, включая Екатеринбургское соглашение от 2009 г., заключенное государствами Шанхайской организации сотрудничества (ШОС) и ратифицированное Казахстаном годом позднее.

Еще одной новацией в рамках Концепции стало диверсифицированное, двоякое понимание информационной безопасности как таковой — в документе это понятие «рассматривается с двух взаимосвязанных аспектов: технического и социально-политического»[15]. Первый, технический аспект вобрал в себя то, что в англоязычных доктринальных документах называется кибербезопасностью (cybersecurity) в ее традиционном понимании. Сюда вошли вопросы защиты информационных систем и инфраструктуры от неавторизованного доступа, использования, раскрытия, нарушения, изменения, прочтения, проверки, записи или уничтожения для обеспечения целостности, конфиденциальности и доступности информации. Выделение такого приоритета в рамках информационной безопасности является своего рода новацией для нормативной системы стран региона. Второй аспект информационной безопасности в рамках Концепции вобрал в себя традиционные вопросы защиты национального информационного пространства и систем распространения массовой информации от деструктивного внешнего информационного воздействия.

Наконец, еще одной особенностью концепции стал выраженный акцент на вопросах киберпреступности, который до этого по большей части отсутствовал либо занимал периферийное место в доктринальных документах Казахстана и государств региона. В общем и целом концепция, хотя и не решила всех теоретических вопросов казахского подхода к обеспечению информационной безопасности, стала явным свидетельством большей *зрелости* национальной модели регулирования инфокоммуникационного сектора.

В Казахстане интернет как неотъемлемая часть глобального информационного пространства давно стал частью жизни общества. Основополагающим принципом государственной политики в области информатизации в Казахстане является развитие в глобальной сети своего собственного сегмента Казнета. Официальная история Казнета имеет своей точкой отсчета 19 сентября 1994 г. — день, когда в базе данных Корпорации Интернета по распределению имен и адресов (The Internet Corporation for Assigned Names and Numbers, *ICANN*) был зарегистрирован домен верхнего уровня .kz. В июне 1995 г. появляется первый каталог казахстанских веб-сайтов — *Kazakh Internet Yellow & White Pages* (ныне уже несуществующий). В декабре 1997 г. был запущен проект наиболее популярного каталога рубрикатора казахстанских веб-ресурсов — *Весь WWW-Казахстан* (*Catalog.Site.KZ*).

Так ко второй половине 1990-х гг. сформировался более-менее цельный национальный сегмент глобальной сети — *Казнет*. Обычно под *Казнетом* понимают совокупность информационных сетевых ресурсов, информационно-телекоммуникационных систем и сетей, технологий их ведения и использования. Все эти информационные системы функционируют на основе единых принципов и общих правил. Основополагающей частью *Казнета* являются веб-сайты, объединяющие следующие типы информационных ресурсов:

- самостоятельные веб-сайты доменной зоны .kz;
- сетевые ресурсы других доменных зон, расположенные на площадках казахстанских провайдеров;
- иностранные сайты, направленные на казахстанскую аудиторию;

- ресурсы казахстанских компаний, расположенные в других доменных зонах[16].

В Казахстане используется трехуровневая система распределенной регистрации доменов (Shared Registry System, SRS) — Регистратура, Регистратор и Регистрант[17]. Управлением и регулированием домена .kz занимаются две организации: Казахский центр сетевой информации *KazNIC*, отвечающий за техническую сторону функционирования домена, и *Казахстанская ассоциация IT-компаний*, в ведении которой находится разработка Правил регистрации и идеология развития национального домена. В настоящее время на рынке регистрации доменов в зоне .kz аккредитовано девять компаний, имеющих статус *Действующий регистратор*. Такая модель подразумевает неограниченное количество регистраторов, имеющих возможность регистрировать доменные имена, используя SRS[18].

Законодательство Казахстана в области интернета в целом находится на промежуточном, не совсем зрелом этапе развития, поэтому государственная политика развития информационного пространства строится исходя из норм и принципов международного права, соблюдения международных договоров и иных актов международного права, ратифицированных в Республике Казахстан в установленном законодательстве порядке, а также с учетом необходимости обеспечения информационной безопасности и защиты законных интересов Республики Казахстан, региональных, местных органов власти, прав физических и юридических лиц. Тем не менее определенная работа в области развития собственного национального законодательства в области интернета в республике проделана. Казахстан — первая страна в Центральной Азии, где были приняты нормативно-правовые документы, регулирующие деятельность участников интернета.

Управление *Казнетом* и координация деятельности различных участников интернет-пространства в Казахстане осуществляется на основе принятой в республике Концепции формирования и развития единого информационного пространства казахстанского сегмента сети интернет (*Казнета*) на 2008–2012 гг. Основная цель Концепции заключается в выработке мер для устойчивого развития единого информационного пространства Казахстана. Для достижения этой цели отмечается необходимость выработки и реализации государственной политики в области развития национального сегмента интернет, совершенствование национального законодательства в области развития национального сегмента интернета, развитие инфраструктуры *Казнета* и обеспечение информационной безопасности. В числе приоритетов также выделяются разработка системы мониторинга и оценки развития единого информационного пространства, участие Казахстана в процессах создания и использования глобальных информационных сетей и систем[19]. Таким образом, Концепция определяет основные направления развития интернета в Казахстане, участников данного процесса, а также меры, способствующие развитию национального сегмента информационного пространства.

Несмотря на определенные позитивные тенденции развития интернета в республике, этот процесс тормозится из-за ряда проблем, препятствующих качественному функционированию *Казнета*. Наличие таких проблем осознают казахстанские законодатели. Одной из них является неразвитость, слабость, несистемное и несвоевременное обновление контента казахских сайтов. Наполнение веб-ресурсов контентом в республике зачастую осуществляется стихийно, в соответствии с интересами и запросами распространителей информации, без должного учета правовых, морально-этических и иных норм, а также национальных интересов. Это ведет к исключению значительной доли сайтов из результатов выдачи крупнейших поисковых систем, включая *Google, Yahoo!, MSN*, а также использующих кириллицу *Yandex, Rambler*. Неудивительно, что в результате доступность и видимость подобных сайтов для пользователей в Казахстане и за его пределами существенно ограничена.

Не менее значимой проблемой для Казахстана является крайне низкий уровень использования государственного языка в *Казнете*. Раньше внедрение казахского

языка сталкивалось с проблемой его кодировки и распознавания, но теперь она решена. Тем не менее казахстанцы используют в основном кириллический контент сайтов. В национальном сегменте Сети почти отсутствуют электронные библиотеки, слабо развиты ресурсы системы образования и науки, мультимедийный контент *Казнета* используется только в части его мобильного применения. Кроме того, в казахской зоне глобальной сети до сих пор нет официального сетевого ресурса, который был бы посвящен использованию государственного языка в органах власти, в повседневной жизни, словарей и глоссария терминов.

Еще одной серьезной проблемой Казахстана в сфере ИКТ является характерное для Центральной Азии в целом информационное неравенство. Не все регионы республики обладают возможностями использования информационных технологий в повседневной жизни. Необходимо отметить, что по состоянию на 2011 г. половина (53,1%) населения Казахстана не имела представления ни об одной из технологий доступа в интернет. Для повышения компьютерной грамотности населения правительство страны в 2006 г. приняло Программу снижения информационного неравенства в Республике Казахстан на 2007–2009 гг. Проблема информационного неравенства связана также с тем, что основной акцент в республики сделан на развитие общенациональных, нежели локальных информационных ресурсов. Подобный подход обусловливает неразвитость местного и регионального информационного рынков и СМИ, отсутствие системной работы на внешнем информационном рынке.

Ведущая роль в разработке и осуществлении национальных программ в области управления интернетом и развитии национального сегмента глобальной сети в Казахстане также принадлежит государству, которое рассматривается как инициатор развития интернета и координатор действий всех участников *Казнета*. В то же время государственные структуры выступают в качестве главного цензора виртуального пространства. К примеру, правительству подконтролен национальный оператор интернет-связи *Казахтелеком*. При этом, однако, государство поощряет участие частного сектора и гражданского общества в консультациях правительства по поводу развития интернет-технологий.

Еще один важный документ, регулирующий функционирование интернета в Казахстане — Концепция развития конкурентоспособности информационного пространства Республики Казахстан на 2006–2009 гг. В концепции анализируются основные проблемы развития информационного пространства в Республике. Основная цель документа сводится к развитию конкуренции между масс-медиа для повышения качества производимого ими информационного продукта; также выявляются ключевые факторы, которые препятствуют конкуренции на казахских информационных рынках. Стимулирование конкурентной среды рассматривается как главная задача государственной политики в информационной сфере.

Следует отметить наличие определенного прогресса в данном направлении. Специфика функционирования информационного пространства Казахстана в том, что, в отличие других государств Центральной Азии, его активными участниками являются не только государство, но и бизнес-структуры, транснациональные компании в области ИКТ, ННО, социально-ориентированные средства массовой коммуникации (СМК) (блоги, социальные сети). Эти участники составляют серьезную конкуренцию государственным информационным системам. Следует выделить деятельность таких электронных СМИ, как *Казахстан, Первый канал-Евразия, Caspionet*. Все данные медиа имеют сайты в интернете, что обусловливает их возросшую популярность. Зона вещания данных медиа-корпораций охватывает не только регион Центральной Азии, но и Средний Восток, Европу и Северную Африку. Специфика взаимодействия государства и ТНК в области ИКТ в Казахстане в том, что они начинают взаимодействовать на уровне национального информационного пространства как равноправные партнеры[20]. Примечателен даже не сам факт подобного взаимодействия, а то, что государство проявляет определенную готовность взаимодействовать с крупными медиа-компаниями как с равными партнерами и делегировать им некоторые свои функции по развитию казахстанского сегмента информационного пространства.

Активным участником информационного пространства Казахстана становятся социальные сети, блоги и веб-платформы, где пользователи могут общаться в режиме онлайн. С 2006 по 2011 г. казахская блогосфера выросла в 3 раза по основным количественным показателям. На сегодняшний день в республике существуют три основных *блог-платформы*: самая популярная *Your Vision*, блоги знаменитостей *Afftor.kz* и блоговая площадка *Blogos.kz.* Среди наиболее популярных социальных сетей следует выделить *Vseti.kz,* практически идентичный российскому *ВКонтакте*. Еще одним популярным порталом является *Liveinternet.kz.* Среди других социально ориентированных веб-ресурсов следует выделить сетевое сообщество *On.kz*, научно-ориентированную социальную сеть Казахстана *Pautina.kz*, казахстанский аналог *Youtube Kiwi.kz*. Помимо активного использования социальных сетей и блогов, использующих собственные платформы, большой популярностью в Казахстане пользуются российские и западные веб-ресурсы. Среди них наиболее востребованными на начало 2012 г. были *Мой Мир* (пользуются 62,4% казахских юзеров), *Одноклассники* (25,9%), *ВКонтакте* (22,7%).

Социальные сети и блоги популярны не только среди казахстанской общественности, но и среди высокопоставленных чиновников. Все члены кабинета министров Казахстана имеют блоги на официальных сайтах своих ведомств, многие ведут аккаунты в *Twitter*. Даже премьер-министр страны Карим Масомов называет себя *активным блогером*. Но, несмотря на видимую *продвинутость* казахских пользователей высших эшелонов власти, социальные сети и блоги вызывают среди них большую настороженность. События в Молдавии весной 2009 г., когда мобилизация масс для антиправительственных акций протеста осуществлялась через социальные сети, блогов, мобильные телефоны, а также череда революций в государствах Ближнего Востока в 2011 г. лишь усилили опасения казахстанских властей в отношении современных интернет-коммуникаций.

24 июня 2009 г. в Казахстане был принят закон «О внесении изменений и дополнений в некоторые законодательные акты по вопросам информационно-коммуникационных сетей». Закон посвящен вопросам регулирования интернета, а потому широкой общественности этот документ известен как закон «Об интернете». В соответствии с законом, все казахские интернет-сайты, включая блоги, чаты и форумы, приравниваются к СМИ, вследствие чего на них — и на их пользователей — распространяется соответствующая уголовная, административная, гражданская ответственность за нарушение казахского законодательства. Примечательно, что под действие закона попадают не только размещенные на интернет-ресурсах материалы, но и комментарии к ним. Владельцы блогов также несут ответственность за информацию и комментарии, размещенные на их страницах. Что касается чатов, то у каждого чата должен быть свой модератор. Вместе с тем, в соответствии с законодательством Республики Казахстан о СМИ, масс-медиа признается таковым, если регистрируется уполномоченным органом и получает лицензию.

Но эти положения не применяются к интернет-ресурсам вследствие отсутствия у последних и регистрации, и лицензии. В данном случае имеет место противоречие в законодательстве. В соответствии с законом «Об интернете», в случае неподчинения решению суда доступ к сайту должен быть заблокирован, а его владелец может лишиться возможности использовать собственный домен и доменные имена с похожими названиями на срок от трех месяцев. За нарушения законодательства суд может заблокировать доступ к ресурсу. Иски в казахские суды можно будет подавать также против размещенных за рубежом сайтов. Между тем, принятие закона «Об интернете» противоречит Концепции формирования и развития единого информационного пространства казахстанского сегмента сети Интернет (Казнета) на 2008–2012 гг. В соответствии с положениями Концепции, правоотношения в интернете носят глобальный характер, а потому применение к ним национальных правовых норм без учета и связи с законодательством других стран может быть неэффективным.

Причиной, побудившей власти Казахстана принять закон об интернете, в значительной степени стала деятельность веб-сайта *Posit.kz*. По мнению казахстанских чиновников, комментарии пользователей ресурса содержали некорректные высказывания и призывы к разжиганию межнациональной и религиозной розни[21]. Ограничения на распространение информации в интернете вводились в Казахстане и ранее — так, в стране неоднократно блокировался доступ к российской блог-платформе *Livejournal*. Еще одной мерой, ограничивающей доступ к интернету, стал приказ Министерства связи и информации от сентября 2010 г. Согласно приказу, компании, использующие казахский интернет-домен (.kz), должны использовать серверное оборудование, физически находящееся на территории Республики Казахстан. Изначально сайты домена .kz размещались на серверах, расположенных за границей, по причине более выгодных цен и лучшего сервиса. Принятие данного приказа было обосновано необходимостью улучшения качества и поддержки казахстанских серверных компаний, но власти это позволяло усилить контроль над *.kz-сайтами*. Под давлением критики, в частности со стороны компании *Google*, в июне 2011 г. госорганами было издано пояснение, согласно которому новые правила касаются *.kz-доменов*, регистрируемых впервые, и не распространяются на уже зарегистрированные доменные имена. Последние, таким образом, получили возможность обновить ежегодную регистрацию, которая по закону необходима для продолжения деятельности веб-ресурсов.

Фильтрация интернет-трафика осуществляется властями Казахстана в основном с помощью доминирующего провайдера телекоммуникационных услуг *Казахтелеком*. Нередки случаи, когда для пресечения работы *неугодного* сайта в республике осуществляются DDoS-атаки. Например, подобной атаке подвергся сайт популярного новостного онлайн-портала *Guljan.org*, что привело к выходу сайта из строя из-за перегрузки его серверов ложными информационными запросами, присланными с зараженных компьютеров. Вскоре после восстановления сайт вновь подвергся аналогичной атаке. Несмотря на то что однозначно ассоциировать подобные атаки с критическим отношением властей к работе тех или иных информационных ресурсов невозможно, именно госструктуры в таких случаях выступают основными объектами подозрений.

УЗБЕКИСТАН

Развитие информационно-коммуникационных технологий занимает важное место в государственной политике Узбекистана**.** Использование в системе государственного и общественного строительства современных ИКТ становится определяющим фактором политической модернизации[22], однако интерпретация термина *информатизация* в сугубо техническом ключе ограничивает его значимость. В Концепции развития информатизации Республики Узбекистан под информатизацией подразумеваются не только организационно-технические и технологические, но и политические, социально-экономические процессы создания условий для удовлетворения потребностей общества с использованием информационных ресурсов, технологий и систем. Целью информатизации называется создание условий для качественного развития национального информационного пространства и формирования в Узбекистане информационного общества[23].

Среди основных участников медиа-пространства республики можно выделить следующих субъектов: государство, неправительственные некоммерческие организации (ННО), частные бизнес-структуры. ННО и бизнес-структуры являются относительно новыми участниками отечественного медиа-рынка, поэтому основная роль модератора процессов информатизации и либерализации СМИ лежит на государстве[24]. Вместе с тем под влиянием геополитических факторов и возрастающих угроз региональной и национальной безопасности государство вынуждено своевременно и адекватно реагировать на них.

Защита информационного пространства от посягательств различных *внешних сил* является составляющей частью проводимой в республике информационной

политики[25]. Однако государство еще не готово к тому, чтобы рассматривать СМИ, принадлежащие частным бизнес-структурам или ННО, как равноправных партнеров. Наблюдается и обратная тенденция: возникающие на медиа-рынке Узбекистана частные СМИ сами не готовы брать на себя такую ответственность, что ведет к недостаточности общественно-политической проблематики в отечественных СМИ и определенной закрытости медиа-пространства к внешнему миру.

Законодательной базой обеспечения информационной безопасности в Узбекистане стал ряд законов, концепций и иных документов, в которых обосновывается необходимость процессов информатизации общества, необходимость защиты информационных ресурсов и обеспечения информационной безопасности[26]. На сегодняшний день нормативно-правовая база Республики Узбекистан характеризуется следующими свойствами:

- содержит четкие определения понятий *информация*, *информатизация*, *информационные ресурсы, национальная информационная система;*
- указывает основные направления государственной политики в сфере информатизации и определяет меры по развитию информационно-коммуникационных технологий в республике;
- определяет механизмы использования и защиты информационных ресурсов;
- упорядочивает принципы формирования национальной политики в области информатизации и телекоммуникаций;
- признает интернет в качестве важного элемента национальной информационной сети.

На практике действия различных субъектов, призванных защищать национальные интересы республики в информационной сфере, не всегда носят упорядоченный характер вследствие того, что понятия *информационная безопасность* и *защита национальных интересов в информационной сфере* еще недостаточно устоялись. Поскольку Узбекистан является участником глобального информационного пространства и развивается в соответствии с мировыми тенденциями в области информатизации, для устойчивого развития необходима Концепция информационной безопасности, которая упорядочивала бы действия всех субъектов информационных процессов в целях защиты от информационных вызовов и угроз современности. В соответствующей концепции следует четко определить базовые понятия, цели, задачи и основные методы защиты национального информационного пространства, выделить и упорядочить действия основных субъектов, ответственных за качественное развитие информационной сферы в стране. Вместе с тем в документе необходимо классифицировать информационные угрозы в военной, политической, экономической, инновационной сферах и выработать необходимые меры защиты.

С учетом того, что тенденции глобализации и информатизации усиливаются, а влияние ИКТ на современные процессы становится одним из факторов развития, целесообразно рассмотреть возможность адаптации нормативно-правовой базы Республики Узбекистан к задачам обеспечения информационной безопасности для защиты национальных интересов страны. Под основополагающими принципами информационной безопасности понимаются доступность, целостность и объективность информации, а не ограничение, запрещение и фильтрация информации. Одной из приоритетных задач для Узбекистана в контексте вызовов безопасности в связи с развитием ИКТ должно стать развитие новых проектов в сфере интернета, которые могут служить интересам национальной и международной безопасности.

Интернет в Узбекистане развивается достаточно динамично. Среди государств Центральной Азии республика занимает первое место по количеству интернет-пользователей, а среди стран СНГ — четвертое. Количество интернет-пользователей по стране составляет 7,55 млн[27]. Эти данные подтверждают, что Узбекистан обладает потенциалом для дальнейшего развития услуг в сфере

интернет-коммуникаций. Одна из основных задач — это расширение географии предоставления интернет-услуг по всей территории страны. Проблема информационного неравенства характерна для Узбекистана, так же как и для других государств. Доступ к интернету имеют лишь 30% населения республики — это в основном жители крупных городов (Ташкент, Самарканд, Бухара). В сельской местности интернет доступен в основном через мобильные телефоны.

Регулирование в области связи, в том числе интернета, осуществляется со стороны Узбекского агентства связи и информатизации (УзАСИ). Агентство обладает нормотворческой инициативой и разрабатывает нормативно-правовые акты, обязательные для исполнения всеми участниками информационного ранка. Акционерная компания *Узбектелеком* является единственным национальным провайдером интернета первого уровня. Через Международный центр пакетной коммутации (МЦПК) *Узбектелеком* предоставляет доступ к интернету другим провайдерам.

Высокая стоимость интернета в Узбекистане — главная причина медленного внедрения интернет-коммуникаций в регионы. Цена обусловлена высокой стоимостью услуг по использованию каналов доступа к международным интернет ресурсам. Например, стоимость аренды канала пропускной способностью до 10 Мбит/с составляет 3,4 тыс. долл. за 1 Мб/с. Подобные тарифы выгодны лишь для операторов и провайдеров, арендующих канал с большой пропускной способностью. Это ведет к олигополии на рынке интернет-услуг. Так, на узбекском рынке интернет-услуг сегодня функционируют четыре крупных провайдера: *UzNet, Sharq Telecom, Sarkor Telecom, TPS*. Они не стремятся развивать интернет услуги в регионах страны по той же причине — дороговизна аренды каналов ведет к дороговизне интернета, что неприемлемо для жителей сельской местности в силу социально-экономических факторов. По сути, *Узбектелеком* должен стимулировать конкуренцию среди провайдеров и создавать условия для появления на рынке новых операторов, что приведет к снижению цен на интернет. Однако на практике нынешняя ситуация олигополии выгодна национальному оператору, так как позволяет регулировать доступ к международным каналам передачи данных.

Самым распространенным методом доступа к интернету остается обычное модемное соединение[28], однако в стране растет количество абонентов, подключенных к интернету по выделенной линии. В 2009 г. их количество составило около 100 тыс. человек. В 2011 г. в столице республики, городе Ташкенте, началось внедрение беспроводного доступа *WiMAX* и оптико-волоконных линий связи. Увеличение количества интернет-пользователей в Узбекистане ведет к росту числа интернет-сайтов в доменной зоне .uz. Домен верхнего уровня .uz был зарегистрирован 29 апреля 1995 г. Правом на управление национальным доменом .uz обладает Центр *Узинфоком*, который является администратором национального домена .uz. В доменной зоне .uz, которую также называют *Узнетом*, аккредитовано семь регистрантов[29]. На начало 2012 г. насчитывается 13,4 тыс. доменов в зоне .uz[30].

Управление зоной .uz имеет свои особенности: так, здесь официально запрещен *кибер*сквоттинг[31]. Кроме того, администрирование доменной зоны ведется полностью открыто — помимо статистики, доступной в режиме реального времени, разные аспекты развития зоны .uz постоянно обсуждаются с заинтересованными пользователями в интернете[32].

Основополагающую роль в развитии интернет-технологий в Узбекистане играет государство. Правоотношения участников интернет-пространства регулируются на основе законов «О связи», «О радиочастотном спектре», «О телекоммуникациях», «Об электронной коммерции» и так далее. Особый акцент в информационной политике Узбекистана сделан на необходимости развития национальной донной зоны .uz. В марте 2012 г. в стране была принята Программа дальнейшего внедрения и развития информационно-коммуникационных технологий в Республике Узбекистан на 2012–2014 гг., где отмечается необходимость развития национального сегмент интернета, в том числе узбекских социальных сетей и других информационных ресурсов[33].

Между тем для *Узнета* характерны все типичные для центральноазиатских государств проблемы в сфере развития интернет-коммуникаций. Первой из них является недостаточная развитость национального сегмента Сети в плане контента, в первую очередь на государственном узбекском языке. Более половины узбекских сайтов (64%) доступны на русском языке и лишь 21% — на узбекском. Наиболее популярными являются новостные сайты: *Gazeta.uz, UzReport.com, Anons.uz, Olam.uz, Vesti.uz, Afisha.uz, Kultura.uz*, посвященные в основном политическим, экономическим, социальным, культурным событиям в жизни республики. Популярность данных интернет-ресурсов обусловлена во многом тем, что размещаемая на них информация, как правило, свободна от влияния государственной идеологии, в отличие от большинства традиционных узбекских масс-медиа. Традиционные печатные и электронные СМИ, а также информационные агентства также имеют свои сайты в интернете, которые позволяют в режиме онлайн узнавать официальную информацию о событиях в Узбекистане. Наиболее популярны Национальное информационное агентство Узбекистана *УзА* (http://www.uza.uz), которое освещает внутриполитическую жизнь республики, и ИА *Жахон* (http://www.jahonnews.uz), повествующее о внешнеполитических сюжетах. Разумеется, в интернете представлены не только национальные СМИ, но и абсолютное большинство структур центральной государственной власти. Наиболее популярной виртуальной площадкой, на которой размещены материалы о правительстве Узбекистана, структуре органов власти Республики, политическом курсе развития страны, нормативно-правовой базе является правительственный портал Республики Узбекистан (http://www.gov.uz).

Наиболее популярными и востребованными населением интернет-ресурсами в Узбекистане, как в большинстве государств региона, являются социальные сети и блоги. При этом максимальная посещаемость узбекских пользователей отмечается в крупнейших трансграничных международных социальных сетях. На *Одноклассниках* зарегистрировано 850 тыс. узбекских граждан, в *Моем Мире* — 625 тыс. человек, владельцами аккаунтов в *Facebook* уже стали более 55 тыс. узбекистанцев, более 1 тыс. человек освоили *Twitter*[34]. Высокой популярностью также пользуется блогплатформа *Lifejournal*. В Узбекистане существует даже ежегодный конкурс «Лучший блогер Узбекистана», что свидетельствует о популярности ведения блогов в республике. Свои страницы в социальных сетях имеют и правительственные учреждения, хотя пока таковых меньшинство. Оппозиционные режиму организации также поддерживают высокую активность в блогосфере и, как правило, ведут страницы в *Facebook*. Однако подобная открытость вовсе не означает, что социальные сети и блоги свободно и беспрепятственно функционируют в Узбекистане.

Оранжевые революции на постсоветском пространстве, *арабская* весна на Ближнем Востоке весьма болезненно воспринимаются властями Узбекистана. Среди политической элиты страны есть осознание, что информационно-коммуникационные технологии, использованные при организации этих событий для мобилизации общественных масс, могут быть применены в деструктивных целях в республике, а потому в Узбекистане осуществляется контроль интернета. Блокирование и фильтрация интернет-сайтов усилилась после событий в узбекском городе Андижане весной 2005 г. Любая информация, содержащая критику в адрес властей, как правило, блокируется. В особой *опале* находятся сайты *Ferghana.ru, Uznews.net, Centrasia.com, Uzmetronom.com.* Некоторые сайты блокируются частично. Социальные сети не подвергаются особой цензуре*: Facebook, ВКонтакте, Одноклассники* функционируют вполне стабильно. Отслеживаются лишь некоторые создаваемые в соцсетях группы, содержащие негативную информацию об Узбекистане. Например, молодежная организация «Етар!» (Хватит! — *пер. с узб.*) посредством социальных сетей и блогов агитировала граждан Узбекистана выйти 1 июня 2011 г. на антиправительственную демонстрацию на площадь Независимости[35] в Ташкенте. В *Facebook* была создана страница этой организации, где осуществлялась мобилизация общественности. Участники группы еще за несколько месяцев до планируемой акции протеста призывали выйти на митинг с запасами еды, постельными принадлежностями, палатками и радиоприемника-

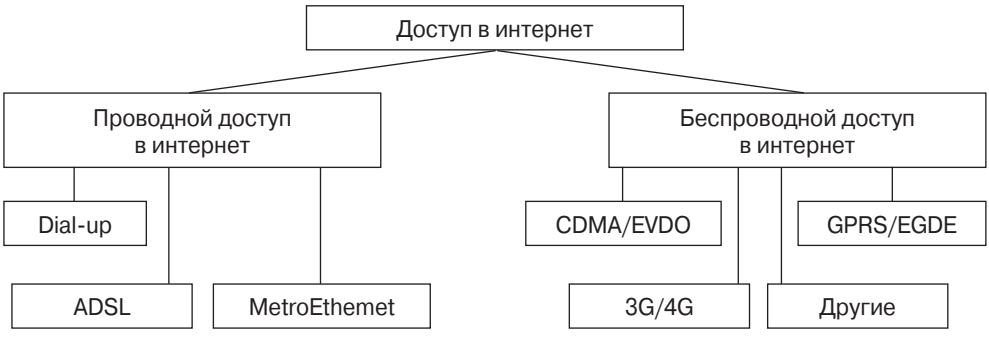
ми[36]. Но демонстрации не состоялись, так как о планируемом мероприятии узнали службы безопасности, которые провели серию разъяснительных мероприятий и призвали граждан, особенно молодежь, не поддаваться на провокации. В стране были усилены меры безопасности, акции не состоялись. Тем не менее эти события показали, что мобилизация масс через социальные сети возможна и в Узбекистане. Эти события повысили бдительность властей по отношению к интернету — усилилась цензура и блокирование сайтов.

Интернет-троллинг — еще один распространенный метод, который власти в Узбекистане используют для контроля контента различных сайтов[37]. Стоит в интернете появиться информации, содержащей критику в адрес властей, действий различных структур правительства, как тут же появляются сотни различных комментариев в их поддержку. Такие комментарии оставляют различные анонимные комментаторы, так называемые *тролли*, специально нанятые правительством для поддержки имиджа и репутации власти. Троллей объединяет анонимность, возможная благодаря интернет-псевдонимам — *никам*. Необходимость в троллинге возникла вследствие того, что даже самые изощренные методы интернет-цензуры, фильтрации, блокирования сайтов не всегда эффективны, в силу различных возможностей обойти запреты в сети можно посредством прокси-серверов. Среди государств Центральной Азии интернет-троллинг активно используют не только в Узбекистане, но и в Казахстане, Таджикистане, Киргизии.

Вместе с тем вероятность мобилизации населения Узбекистана через интернет-коммуникации по арабскому сценарию остается весьма низкой. Основными причинами являются информационное неравенство и ограниченный доступ к интернету у большей части населения республики. В сельских областях Узбекистана ограничен также доступ к зарубежным СМИ. Местные СМИ не информируют жителей о событиях в мире в должной мере (например, узбекские СМИ не сообщают о событиях так называемой *Арабской весны*). К тому же жители, имеющие доступ в интернет, осознают, что власти контролируют интернет-пространство, и избегают активного участия в обсуждениях внутриполитических событий.

Однако блокировка сайтов далеко не всегда оказывается эффективным инструментом. В Узбекистане активно используются прокси-серверы, позволяющие открывать все запрещенные сайты. К тому же отслеживать и фильтровать всю информацию, публикуемую в социальных сетях и блогах, которые созданы на платформах зарубежных государств, не всегда осуществимо практически. Для повышения уровня нравственности и общественной морали в Узбекистане начали создаваться собственные социальные сети. Первой национальной социальной сетью в республике стала сеть *Muloqot* [Общение. — *пер. с узб.)*], запущенная 1 сентября 2011 г. Площадка рассчитана в основном на молодежь. Чтобы стать участником сети, необходимо пройти процедуру регистрации, важным условием которой является сообщение номера сотового телефона пользователя. Такая опция позво-

Рис. 1. **Способы доступа в интернет в государствах Центральной Азии**



ляет разработчикам сайта связаться с пользователем в случае нарушения условий общения в социальной сети, а значит, контролировать все действия не *виртуальных*, а реальных пользователей. *Muloqot* функционирует на узбекском и на русском языках. Количество зарегистрированных пользователей к началу 2012 г. составляло 20 тыс. человек. Однако этой социальной сети достаточно сложно конкурировать с *Facebook, ВКонтакте, Одноклассники* и завоевывать новых пользователей.

КИРГИЗИЯ

Информационно-коммуникационная инфраструктура Киргизии развивается достаточно динамично, в целом этот процесс соответствует глобальным тенденциям развития информационного пространства. Оговорку стоит сделать в отношении вопросов обеспечения информационной безопасности, которые пока не получили концептуального закрепления на доктринальном и нормативно-правовом уровне, хотя и затрагиваются в ряде документов[38]. В частности, в республике на данный момент отсутствует единая концепция информационной безопасности. Между тем внутриполитические реалии, нестабильность политической системы, проблемы социально-экономического характера ведут к росту внешних угроз, которые заявляют о себе прежде всего через информационное пространство. События лета 2010 г. показали, что столкновения между политическими силами внутри страны и межэтнические столкновения между диаспорами находят активное отражение в информационном пространстве. Республиканские СМИ стали участниками противостояний, однако не всегда могли отразить информационные атаки западных и региональных СМИ. Это происходит в силу того, что в отличие от соседних республик, Киргизия не является центральным участником медиа-пространства Центральной Азии и далеко не всегда способна своевременно реагировать на процессы, протекающие в нем. Общественность страны давно начала обсуждать проблемы государственной политики в области обеспечения информационной безопасности, поскольку обилие нормативно-правовых документов в области информатизации, СМИ и телекоммуникаций ведет к неоднозначному толкованию многих терминов и определений, а разрозненность субъектов информационного рынка, ответственных за обеспечение информационной безопасности, мешает проведению четкой политики в этой сфере. Таким образом, создание единого концептуального документа должно прояснить суть многих терминов в сфере информатизации, упорядочить субъектов информационной деятельности и определить методы обеспечения безопасности информационной сферы.

Вместе с тем Киргизия опережает соседние государства Центральной Азии по темпам развития интернета. Количество интернет-пользователей превысило 2 млн человек, что составляет 39% населения. Но доступ к интернету имеют лишь крупные города страны, такие как Бишкек, Ош, Джалал-Абад. Активное внедрение интернет-технологий происходит в основном за счет мобильной связи, посредством которой 20% пользователей от общего числа имеют доступ к глобальной сети. В отдаленных регионах Киргизии интернет не развит в силу слабой компьютеризации и снижения уровня владения русским языком (который составляет основу киргизского сегмента интернет-пространства). Проблема информационного неравенства решается за счет некоторых зарубежных структур, которые за счет собственных средств создают в отдаленных регионах информационные ресурсные центры, где для жителей имеется бесплатный доступ в интернет. Мобильная связь, через которую жители отдаленных регионов Киргизии получают доступ в интернет — еще одни способ для преодоления проблемы информационного неравенства в республике. Мобильная связь доступна 6 млн жителей республики, или 90% населения[39].

Национальным оператором интернет-услуг является *ОАО Кыргызтелеком*. Однако на рынке существует более 37 частных интернет-провайдеров, которые составляют серьезную конкуренцию государственному оператору. Среди наиболее крупных частных компаний, предоставляющих услуги интернет, следует выделить *ElCat* и *Saima Telecom Aknet*. Эти компании обладают большими по сравнению с *Кыр-*

гызтелекомом, финансовыми и человеческими ресурсами, необходимыми для расширения и развития интернет-услуг. Подобная ситуация вынудила правительство Киргизии приватизировать *Кыргызтелеком*. 27 марта 2012 г. компания была выставлена на продажу[40].

Несмотря на обилие провайдеров, стоимость доступа в интернет в Киргизии достаточно высока. Причины те же, что и в Узбекистане — высокая цена за аренду магистральных каналов у иностранных интернет-операторов, невысокий платежный потенциал клиентов. Доступ в интернет по-прежнему лимитируется. Безлимитные тарифы и высокую скорость трафика могут позволить себе лишь корпоративные клиенты. В 2009 г. на юге Киргизии начала функционировать волоконно-оптическая линия связи (ВОЛС), проложенная через Таджикистан и Китай. Доступ к интернету через эти страны, особенно через Китай, привел к некоторому снижению цен на интернет. Тем не менее ВОЛС не соединена с севером страны, где расположен главный *потребитель интернет-услуг* — Бишкек.

За Киргизией закреплена доменная зона .kg, зарегистрированная в 1995 г. Количество доменов первого уровня, зарегистрированных в настоящее время в зоне .kg, не превышает четырех тысяч. Невысокая популярность национального домена обусловлена его высокой стоимостью. Цена домена в зоне .kg составляет 50 долл., в то время как стоимость доменов .com, .net, .org, .ru, .info составляет 7 долл. Администрированием зоны .kg занималась компания *АзияИнфо*, которой делегировала соответствующие полномочия ICANN. Однако в 2009 г. право на администрирование национальной доменной зоны было передано Государственной патентной службе *Кыргызпатент*[41]. Решение принял президент Курбанбек Бакиев, который посчитал, что доменная зона, которая обозначается международным кодом государства, является его национальным достоянием, а потому управление ей должны осуществлять государственные органы[42]. Смена частного администратора зоны .kg на государственного привела к усилению контроля над интернетом в республике.

Большинство действующих в зоне .kg сайтов русскоязычные. Контент на киргизском языке достаточно слабо развит и практически не сформирован в единую систему информационных ресурсов. Вместе с тем большинство национальных СМИ имеют собственные сайты в интернете и достаточно активно используют их. В соответствии с законодательством Киргизии, веб-сайты не являются СМИ, вследствие чего они не подпадают под соответствующее правовое регулирование. Неясный правовой статус таких ресурсов делает их своеобразным инструментом ведения локальных информационных войн, информационных кампаний. В частности, интернет активно используется оппозицией для обозначения своих целей, критики власти и даже для призывов своих сторонников к активным действиям. Эта практика существовала как во времена экс-президента Акаева, так и при режиме Бакиева. Наиболее популярными СМИ в интернете являются информационный сайт *Vesti.kg*, аналитические порталы *Comment.kg, 24kg, Kabar.kg, Parus.info*. На киргизском языке наиболее популярна газета *Супер Инфо* и радио *Аззатык*. Популярность и востребованность этих ресурсов обусловлена относительно объективной и своевременной информацией. К тому же киргизские масс-медиа часто публикуют оппозиционные по отношению к действующей власти материалы, которые пользуются спросом среди сторонников оппозиции и внешней аудитории, следящей за ситуацией в стране.

В годы правления Курманбека Бакиева в республике имели место попытки ограничить свободу слова в СМИ и интернете: осуществлялись блокирование, фильтрация сайтов, ограничение на анонимные комментарии пользователей на сайтах СМИ. Тем не менее интернет был и остается для граждан Киргизии самым свободным местом для самовыражения. В преддверии государственного переворота в Киргизии весной-летом 2010 г. через интернет распространялась жесткая критика в адрес правительства и президента, что стало существенным элементом в подготовке общественного сознания к свержению Бакиева. Особую роль в мобилизации общественных масс для совершения государственного переворота сыграли социальные сети и блоги. По данным Национального статистического

комитета Киргизии, более 900 тыс. жителей Киргизии зарегистрированы в таких социальных сайтах, как *Twitter, Facebook, ВКонтакте, Мой Мир* и *Одноклассники*. Это довольно внушительная часть населения для страны с населением 5,4 млн человек. Страницы в социальных сетях имеют многие активные участники общественного и политического процесса, в том числе депутаты, общественные деятели и правозащитники. Местных, равно как и национальных социальных сетей, в Киргизии практически нет. Зачастую для массового обмена информацией помимо международных социальных сетей, используются форумы, а также блоговые платформы некоторых популярных информационных сайтов. Наиболее популярным политическим форумом считается *Diesel Forum*, который активно используется для освещения обсуждения массовых акций в предвыборной борьбе. К январю 2012 г. на форуме были зарегистрированы около 70 тыс. пользователей.

В то же время социальные сети, блоги и интернет-форумы сыграли важную роль в оказании помощи пострадавшим в ходе этнических столкновений между киргизской и узбекской диаспорами на юге страны. Сетевые интернет-коммуникации зачастую доводили и распространяли информацию о событиях более оперативно по сравнению с информагентствами. С помощью социальных сетей и блогов были организованы добровольные народные дружины для оказания помощи пострадавшим. Примечательно то, что на призывы об оказании гуманитарной помощи откликнулись не только киргизские блогеры, но и блогеры из Узбекистана, Казахстана, Таджикистана.

ТУРКМЕНИСТАН

В Туркменистане сфера информационно-коммуникационных технологий получила развитие после прихода к власти в 2007 г. президента Гурбангулы Бердымухамедова. В республике появился интернет, определенный импульс к развитию получили СМИ. До этого в Туркменистане функционировали лишь государственные СМИ, которые были практически полностью закрыты от внешнего мира и не представлены в глобальном информационной пространстве. Подобный формат развития масс-медиа определялся *принципом нейтралитета*, которого придерживалось руководство республики. Однако с приходом нового руководства Туркменистана обозначился новый вектор развития страны и наметились некоторые сдвиги в национальной модели регулирования масс-медиа. Огромные запасы туркменского природного газа привлекают в страну иностранных инвесторов, проявляющих интерес к различным энергетическим проектам. Власти осознают, что взаимодействие со стратегическими инвесторами требует более широкой представленности страны в глобальном информационном пространстве, поэтому предпринимают попытки развивать медиа-сферу Туркменистана, включая ее онлайн-сегмент.

Нормативно-правовая база Туркменистана до недавнего времени основывалась на законодательной базе бывшего СССР. До сих пор действует закон «О печати и других средствах массовой информации в Туркменской ССР», который регулирует правовые отношения в области получения и распространения информации[43]. В законе, объективно не соответствующем реалиям времени, не отражены даже элементарные понятия в области информатизации.

Осознавая новые реалии, правительство страны стремится ускорить разработку и принятие нормативно-правовой баз за счет принятия ряда более актуальных нормативно-правовых актов[44]. Вместе с тем в законодательной базе Туркменистана до сих пор отсутствует определение понятия *информационной безопасности*, не обоснована значимость данной проблемы для дальнейшего развития Туркменистана как полноправного субъекта международных отношений. Представляется, что опыт других государств в сфере обеспечения информационной безопасности может быть весьма полезен для Туркменистана.

Смена власти в стране привела еще к одному важному событию, несколько ускорившему развитие ИКТ в республике. Президентство Гурбангулы Бердымухаме-

дова ознаменовалось, без явных преувеличений, появлением в стране интернета. Хотя национальный домен .tm был зарегистрирован в 1997 г., его активное использование и развитие на практике началось лишь спустя десятилетие. В 2007 г. в Туркмении появились первые интернет-кафе и *ресурсные центры*, где жители страны могли освоить азы пользования интернетом. По состоянию на июнь 2012 г. общая численность интернет-пользователей в Туркмении составляла 120 тыс. человек, а количество доменных имен, зарегистрированных в зоне .tm, — 3,8 тыс.[45]. Однако это количество обусловлено тем, что национальный домен Туркмении совпадает с общепринятым обозначением товарного знака ТМ, и возникла идея продать иностранным компаниям домены .tm. Но зона была заморожена, а право зарегистрировать в ней домен, и то только третьего уровня, получили лишь жители и организации Туркмении. Открытая регистрация была возобновлена в 2003 г. и стала доступна для всех физических и юридических лиц, что позволило властям сделать из продажи доменов бизнес. Но из-за низкого уровня соединения, тотального контроля правительства, высокой стоимости домена, составляющей 1 тыс. долл., желающих получить домен на зоне .tm немного[46].

Туркмения остается одним из наиболее закрытых государств по отношению к интернету. Главным монополистом по предоставлению интернет-услуг является государство и действующий от его лица оператор — компания *Туркментелеком*. Помимо национального оператора в стране действовала российская компания *Мобильные ТелеСистемы (МТС)*, которая наряду с предоставлением услуг сотовой связи, начала предоставлять услуги доступа в интернет. Однако деятельность операторов интернета, равно как и сам контент, тщательно контролируется властью. Государство контролирует выдачу лицензий независимым интернет-провайдерам, считая, что это может нести угрозу безопасности. Соответственно, любой сайт, где единожды прозвучала критика туркменских властей, моментально блокируется для доступа с территории Туркменистана. Это касается сайтов газет и журналов, в первую очередь российских, а также сайтов международных правозащитных организаций, сайтов радиостанций *Би-Би-Си*, *Немецкая волна*, сайтов радиостанций *Голос Америки*, *Свобода*, туркменской службы *Радио Свобода*, сайтов туркменских оппозиционных и диссидентских организаций за рубежом. Наряду с блокированием сайтов спецслужбы страны ведут мониторинг попыток посещений тех или иных сайтов, ни и, разумеется, контроль личной переписки пользователей. Особая процедура контроля за доступом в интернет существует и в интернет-кафе. Каждый посетитель должен предъявить документ, удостоверяющий личность. Стоимость интернет-услуг в стране в несколько раз превышает тарифы в соседних государствах региона[47].

Контент на туркменском языке практически не развит. Социальные сети и блоги не получили в стране развития в силу того, что власти запрещают их функционирование в стране и блокируют доступ к ним. Тем не менее в стране наметилась тенденция в сторону создания собственных национальных социальных сетей, блогов и форумов. Форум *Teswirlar.com* и блоговая площадка *Talyplar.com* наиболее популярны среди туркменских интернет-пользователей и представителей туркменской диаспоры за рубежом[48].

В Туркмении фактически не существует независимых, частных СМИ, в том числе в интернете. Любые публикации проходят проверки у государственных чиновников. Контроль материалов в интернете усилился в 2011 г. после взрывов на складе боеприпасов в Абадане. Тогда власти старались не допустить распространения этой информации вовне, но произошла утечка, и зарубежные СМИ обрушились с критикой на власти Туркмении, предположительно допустивших инцидент с массовыми человеческими жертвами. Спецслужбы Туркмении пытались выявить лиц, подозреваемых в передаче информации о взрывах иностранным СМИ посредством интернета и сотовой связи. Базирующийся в Австрии веб-сайт Туркменской инициативы по правам человека подвергся хакерской атаке после публикации статей о взрывах. Корреспондента *Радио Свободы*, написавшего о взрывах в блоге, посадили в тюрьму по сфабрикованному уголовному обвинению; позже

он был освобожден по амнистии. Началась новая кампания против спутниковых антенн, одних из немногих оставшихся средств получения независимой информации в стране.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦЕНТРАЛЬНОЙ АЗИИ ПОД ЗАЩИТОЙ ШОС, ОДКБ, СНГ

Анализ подходов государств Центральной Азии к обеспечению информационной безопасности и управлению интернетом показал, что каждая республика региона самостоятельно формирует подходы к решению этих вопросов. Несмотря на схожесть методов, используемых республиками в преодолении проблем информационного неравенства, развития национального сегмента в интернете, формировании нормативно-правовой базы в области информационной безопасности, отсутствуют единые региональные подходы для решения этих проблем. Это происходит вследствие достаточно сложных и зачастую противоречивых отношений между государствами Центральной Азии, обусловленных различным характером внутри- и внешнеполитического развития государств региона. Существовавшая внутри региона организация *Центрально-Азиатское сотрудничество*, объединявшая республики в единый интеграционный блок и регулировавшая проблемы внутри региона, прекратила свое существование в 2005 г. и была объединена с ЕврАзЭС.

По мере возрастания глобальных информационных угроз, представляющих опасность государственной целостности и стабильности, центральноазиатская политическая элита осознает, что меры, принимаемые на уровне одного государства, не всегда эффективны и достаточны. Транснациональный характер развития информационного пространства обусловливает трансграничность вызовов и угроз. Следовательно, для обеспечения информационной безопасности в рамках даже одного государства необходимо принятие единых региональных или глобальных мер. Государственные перевороты на постсоветском пространстве, *Арабская весна* на Ближнем Востоке привели к пониманию лидерами государств Центральной Азии необходимости сообща решать вопросы в области обеспечения информационной безопасности.

Одной из площадок, где началось активное обсуждение вопросов международной информационной безопасности (МИБ) с участием центральноазиатских государств, стала ШОС, членами которой являются, в том числе, государства Центральной Азии. В 2006 г. на саммите организации в Шанхае вопросы информационной безопасности были впервые обозначены в повестке дня. По итогам саммита было принято «Заявление глав государств — членов ШОС по международной информационной безопасности», где подчеркивалось, что в современном мире ИКТ могут быть использованы в преступных, террористических и военно-политических целях, что представляет угрозу для международной безопасности и способно дестабилизировать общественную жизнь государств.

Для противодействия информационным угрозам была создана группа экспертов государств — членов ШОС по вопросам МИБ. Актуальность проблем обеспечения МИБ как одного из ключевых элементов общей системы международных отношений подчеркивается в Екатеринбургской декларации ШОС, принятой государствами-членами в ходе саммита организации в России в 2000 г.[49]. В Ташкентской декларации ШОС, принятой в 2010 г. в ходе саммита организации в Узбекистане, информационная безопасность также рассматривается как важный фактор обеспечения государственного суверенитета, национальной безопасности, социально-экономической стабильности[50].

Еще одним способом противодействия информационным угрозам стала озвученная в Узбекистане в 2007 г. инициатива создания единого информационного пространства ШОС[51]. Это пространство, по мнению сторонников идеи, призвано способствовать формированию единых культурных и нравственных ценностей у населения стран ШОС. Для этой цели предполагалось унифицировать право-

вое регулирование отношений в информационной сфере, а также средства поиска, сбора, хранения, анализа и защиты информации в государствах, входящих в состав организации.

Не менее важными задачами на пути создания единого информационного пространства ШОС рассматривались формирование и реализация согласованной политики в области развития СМИ и интернет-коммуникаций. Однако в государствах — членах организации уже сформировались различные модели информационного пространства, зачастую используются диаметрально противоположные методы и инструменты развития сферы ИКТ, контрастируют культурно-ценностные установки, пропагандируемые в СМИ, различаются национальные подходы к вопросам информационной безопасности и управлению интернетом. В силу этих причин формирование единого информационного пространства в рамках ШОС представляется не самой актуальной и легко осуществимой задачей.

В сентябре 2011 г. государства, входящие в состав ШОС, в частности Россия, Китай, Таджикистан и Узбекистан, внесли на рассмотрение Генеральной Ассамблеи ООН международный проект в области МИБ. В письме постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при ООН от 12 сентября 2011 г. на имя Генерального секретаря государства, подписавшие документ, разработали и предложили так называемые Правила поведения в области обеспечения МИБ[52]. Документ регулирует действия государства в информационном пространстве, в частности, отмечается недопустимость использования ИКТ в целях, противоречащих обеспечению международной безопасности. Правила призывают государства-члены ООН к сотрудничеству в борьбе с преступной или террористической, экстремистской деятельностью с использованием информационных средств, а также деятельностью, подрывающей политическую, экономическую и социальную стабильность государств, их культурный и духовный уклад.

В документе отмечается необходимость создания многосторонних и демократических механизмов управления интернетом, способствующих его безопасному и стабильному функционированию. В нем также предлагается ввести запрет на использование интернета в военных целях, при этом наделить правительства свободой действий внутри национальных сегментов интернета[53]. Но Правила поведения, предложенные Россией, Китаем, Узбекистаном и Таджикистаном, пока не нашли достаточно широкой поддержки среди делегатов Генеральной Ассамблеи ООН. Критическую позицию по отношению к документу заняли США и их западные партнеры, расценивающие предложенные в проекте документа механизмы как попытку установить государственный контроль над интернетом[54].

Еще одной региональной структурой, включающей государства Азии и акцентирующей внимание на вопросах информационной безопасности, является Организация Договора о коллективной безопасности (ОДКБ). Сотрудничество в этом направлении в рамках ОДКБ началось в сентябре 2008 г., когда была утверждена Программа совместных действий по формированию системы информационной безопасности государств — членов организации. Программа охватывает такие важные направления, как сотрудничество в политической сфере, формирование согласованной нормативной правовой базы, совместные научные и исследовательские работы, обмен информацией о достижениях в этой области, подготовка кадров, обеспечение безопасности критически важных объектов проведение совместных мероприятий. Особое внимание в документе уделяется разработке единого понятийного аппарата в сфере информационной безопасности, совместному противодействию информационным угрозам, взаимодействию спецслужб и правоохранительных органов в сфере обеспечения защиты секретной информации, а также противодействие иностранным техническим разведкам[55].

В 2010 г. ОДКБ приняла Положение о сотрудничестве в сфере информационной безопасности. Основная цель утвержденного документа — это формирование организационных и правовых основ сотрудничества в государствах — членах организации. В целях противодействия преступлениям в сфере информационных

технологий ОДКБ проводит операцию ПРОКСИ[56]. Основная цель операции — противодействие киберпреступлениям в государствах — членах организации и распространению в интернете информации, наносящей политический ущерб национальным и союзническим интересам[57]. Важной задачей ОДКБ стала подготовка кадров в области информационной безопасности.

Вопросы обеспечения информационной безопасности также находятся в центре внимания Содружества Независимых Государств (СНГ). В 2008 г. были приняты Концепция сотрудничества государств — участников СНГ в сфере обеспечения информационной безопасности и Комплексный план мероприятий по реализации данной концепции на период с 2008 по 2010 г.[58]. В документах классифицируются виды информационных угроз, причем особый акцент сделан на недопущение проведения третьими странами в информационном пространстве мероприятий, направленных на дестабилизацию социально-политической обстановки в государствах — участниках СНГ. В Концепции выделяют правовые, организационно-технические и организационно-экономические методы обеспечения информационной безопасности, а также звучит призыв повысить ответственность государств за процессы информатизации и развитие интернет-коммуникаций.

Анализ доктринальных документов таких региональных структур, как ШОС, ОДКБ, СНГ, по вопросам информационной безопасности показывает, что ведущая роль в процессах информатизации закреплена за государством. Понятие «информационная безопасность» в основном интерпретируется как защита и закрытие информационной инфраструктуры государств — участников организаций от внешних негативных воздействий. Как представляется, такое понимание в значительной степени противоречит подходу, в рамках которого делается акцент на доступность, целостность, объективность информации.

ЗАКЛЮЧЕНИЕ

На основе анализа подходов государств Центральной Азии к вопросам информационной безопасности и управлению интернетом можно сделать общий вывод о том, что проработка данной проблематики в рамках государственной политики стран региона пока еще находится в довольно ранней промежуточной стадии. Каждая республика стремится формировать собственные подходы к обеспечению информационной безопасности, которые находят отражение в национальных законодательствах. В республиках создаются специальные комиссии по проблемам информационной безопасности, принимаются межправительственные соглашения по защите информационного пространства. Однако следует признать, что на теоретическом и доктринальном уровнях упомянутые проблемы преимущественно не проработаны.

Характерным примером является устойчивое воспроизведение в законодательстве центральноазиатских республик подхода, в рамках которого под информационной безопасностью понимается защита национального информационного пространства от деструктивного воздействия *внешних сил*. При этом за негативное внешнее влияние власти часто принимают любую информацию, содержащую критику в адрес правительства и других структур власти. В то же время недостаточное внимание при таком подходе уделяется вопросам управления интернетом. Несправедливо утверждать, что ситуация не меняется — обновление доктринальной основы политики в области информационной безопасности в Казахстане стало неплохим примером позитивной динамики. Кроме того, такой подход в значительной мере одновременно является *проекцией* и базой для того видения данных вопросов, которое доминирует в рамках региональных организаций, объединяющих большинство центральноазиатских республик — Организации Договора о коллективной безопасности (ОДКБ) и ШОС. Таким образом, государства региона частично решают задачу обеспечения единства своих подходов к вопросам информационной безопасности, однако частично это происходит в ущерб глубине и охвату последних. Представляется, что по мере качественного развития нацио-

нальных ИТ-секторов и выхода на первый план таких проблем, как безопасность критической инфраструктуры, киберпреступность и др., существующие доктринальные подходы потребуют модернизации и частичного пересмотра.

Как было показано выше, во всех без исключения государствах Центральной Азии ведущую роль в процессах информатизации играет государство. Государственные структуры регулируют развитие интернет-коммуникаций и контролируют деятельность частных интернет-провайдеров. Кроме того, в государствах региона — за некоторыми оговорками в отношении Киргизии — достаточно ярко выражена *интернет-цензура*. Власти достаточно регулярно осуществляют фильтрацию и блокирование *неугодных* сайтов. Как правило, под такие меры подпадают интернет-ресурсы, содержащие критику в адрес политического руководства или государственного устройства страны. Высокая стоимость интернета, неразвитость инфраструктуры и, как следствие, проблема информационного неравенства входят в число основных проблем, препятствующих полноценному развитию и более широкому проникновению интернета в государствах Центральной Азии. Некоторые шаги в сторону либерализации рынка интернет-услуг за последние годы были сделаны в Казахстане и Киргизии.

Еще одним приоритетным направлением для государств региона является развитие собственных национальных доменов. Однако систематизированный контент на государственном языке окончательно не сформирован ни в одной стране региона. Большинство сайтов, зарегистрированных на национальных доменах, функционируют на русском языке. Еще одной причиной неразвитости контента на государственных языках является высокая стоимость регистрации доменов в национальной зоне.

Социальные сети и блоги пользуются большой популярностью практически во всех государствах региона. Новые электронные формы массовой коммуникации становятся площадкой, где граждане могут относительно свободно и беспрепятственно высказывать свое мнение по злободневным проблемам внутриполитического развития, что зачастую вызывает большую озабоченность властей. Правительства государств Центральной Азии рассматривают контроль и регулирование социальных сетей и подобных им сервисов в качестве одного из приоритетных направлений в области информационной безопасности. Однако популярность создаваемых в государствах региона социальных сетей ниже, чем популярность *Facebook, Twitter, ВКонтакте, Одноклассники, Мой Мир*.

На региональном уровне государства Центральной Азии стремятся решать проблемы в области информационной безопасности в рамках различных интеграционных структур, в основном в рамках ШОС, ОДКБ, СНГ. Подход этих структур в основном заключается в повышении ответственности государства за развитие информационных процессов и защиты от негативного информационного воздействия извне.

В этом свете надо понимать, что успешное развитие национальных сегментов интернета в государствах региона во многом зависит от того, пойдут ли власти центральноазиатских республик на дальнейшую либерализацию сектора ИКТ и удастся ли им совместить подобную политику с обеспечением информационной безопасности. Перед государствами Центральной Азии стоит задача не столько *экстенсивного* расширения собственных национальных сегментов Сети — глобализация, экономический рост и диффузия технологий сделают это за них, сколько их *качественного совершенствования* и обеспечения их конкурентоспособности в мировом информационном пространстве. Приоритетом должно стать развитие новых проектов в области интернета, в частности социально ориентированных площадок, интерактивных платформ и онлайн-проектов. Движение в этом направлении может не только не противоречить, но и напрямую служить интересам национальной и международной безопасности за счет беспрецедентного расширения потенциала интерактивного взаимодействия государственных органов с населением, информирования, оповещения и мониторинга — как государственного, так и общественного.

Примечания

[1] В настоящей статье под Центральной Азией понимается регион, объединяющий пять постсоветских республик: Казахстан, Узбекистан, Киргизию, Таджикистан и Туркмению.

[2] Asia Internet Use, Population Data and Facebook Statistics. Internet World Stats. 2011. 31 декабря. http://www.internetworldstats.com/stats3.htm#asia (последнее посещение — 26 августа 2012 г.).

[3] Интернет в Центральной Азии: обычное средство связи или роскошь? *Информационное агентство Фергана.news*. 2003. 7 марта. http://www.fergananews.com/article.php?id=1456 (последнее посещение — 27 августа 2012 г.).

[4] В интернете троллями называют лиц, провоцирующих эмоциональную перепалку, преследующих других пользователей или выдающих себя за других людей. Это слово изначально происходит не от названия от мифологических троллей, а от рыболовного термина троллинг (англ. trawling — ловля на блесну), но созвучие так прижилось, что отождествление интернет-хулиганов с троллями стало общим местом и даже темой для шуток и карикатур.

[5] Концепция информационной безопасности Республики Таджикистан. *Национальная ассоциация независимых СМИ Таджикистана*. 2003. 7 ноября. http://www.nansmit.tj/laws/?id=26 (последнее посещение — 26 августа 2012 г.).

[6] Там же.

[7] Законодательство о СМИ стран Центральной Азии (Таджикистан). *Право и СМИ в Центральной Азии*. 2011. 10 апреля. http://medialaw.asia/legislation/38/21 (последнее посещение — 26 августа 2012 г.).

[8] История печатных СМИ Таджикистана: от зависимых до «независимых». *Сто сторон*. 2011. 17 ноября. http://www.100 storon.ru/smi_20_years/20111116/249602764.html (последнее посещение — 27 августа 2012 г.).

[9] Таджикистан остался без Facebook. *Internet–Technologies*. 2012. 5 марта. http://www.internet–technologies.ru/news/news_2343.html (последнее посещение — 26 августа 2012 г.).

[10] Таджикистан блокирует Facebook и другие неугодные сайты. *Русская служба BBC*. 2012. 5 марта. http://www.bbc.co.uk/russian/mobile/international/2012/03/120305_tajikistan_internet_ban.shtml (последнее посещение — 26 августа 2012 г.).

[11] Концепция информационной безопасности Республики Казахстан. *Право и СМИ в Центральной Азии*. 2007. 5 апреля. http://www.medialawca.org/document/–1234 (последнее посещение — 26 августа 2012 г.).

[12] См. подробнее: Законодательство о СМИ стран Центральной Азии (Казахстан). *Право и СМИ в Центральной Азии*. 2010. 23 ноября. http://medialaw.asia/legislation/36/21 (последнее посещение — 26 августа 2012 г.).

[13] См.: Концепция информационной безопасности Республики Казахстан. *Право и СМИ в Центральной Азии*. 2007. 5 апреля. http://www.medialawca.org/document/–1234 (последнее посещение — 26 августа 2012 г.).

Также см.: О Концепции формирования и развития единого информационного пространства казахстанского сегмента Интернет на 2008–2012 гг. *Право и СМИ в Центральной Азии*. http://medialaw.asia/document/–1009 (последнее посещение — 26 августа 2012 г.).

[14] Указ президента Республики Казахстан от 14.11.2011. № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 г.». *Nomad*. 2011. 6 декабря. http://www.nomad.su/?a=3–201112060038 (последнее посещение — 27 августа 2012 г.).

[15] Там же.

[16] Концепция формирования и развития единого информационного пространства казахстанского сегмента сети интернет (Казнета) на 2008–2012 гг. Международный казахский сервер Казах.ру. 2008.12 мая. http://www.kazakh.ru/news/articles/?a=1274 (последнее посещение — 27 августа 2012 г.).

[17] *Регистратура* — организация, определяемая администратором доменного имени KZ по согласованию с уполномоченным органом и международной организацией ICANN (Internet Corporation for Assignet Names and Numbers), осуществляющая ведение реестра доменных имен KZ в сети Интернет.

Регистратор — юридическое лицо, резидент Республики Казахстан, аккредитованное администратором доменного имени KZ, оказывающее услуги регистрантам по регистрации доменного имени, обеспечивающее внесение в реестр необходимой информации в соответствии с Соглашением (Договором), заключенным между регистратурой и регистратором и реализующее права регистранта по управлению доменным именем в регистратуре.

Регистрант — физическое или юридическое лицо, направившее регистратору заявку и необходимые для регистрации (продления, изменения, передачи, трансфера, отмены) доменного имени документы и являющееся его владельцем на период регистрации, обладающее правами и обязанностями по управлению сведениями о зарегистрированном доменном имени.

См. подробнее: Порядок внедрения домена «.КАЗ». Казахский центр сетевой информации. 2012. январь 30. http://www.nic.kz/docs/poryadok_vnedreniya_kaz_ru.pdf (последнее посещение — 27 августа 2012 г.).

[18] Доменная зона KZ, регистрация доменов KZ. Сервис регистрации доменных имен General–Domain.Ru. http://www.general–domain.ru/katalog/kz.php (последнее посещение — 27 августа 2012 г.).

[19] Концепция формирования и развития единого информационного пространства казахстанского сегмента сети Интернет (Казнета) на 2008–2012 гг. Министерство экономического развития и торговли Республики Казахстан. 2008, 7 июля, http://www.minplan.kz/economyabout/358/1312 (последнее посещение — 27 августа 2012 г.).

[20] TNS Central Asia измерили медиа-рынок Казахстана: *Русское Радио* лидирует. *Радио Портал*. 2010, 10 июня, http://www.radioportal.ru/articles/9479/tns–central–asia–izmerili–mediarynok–kazakhstana–russkoe–radio–lidiruet (последнее посещение — 27 августа 2012 г.).

[21] Премьер Казахстана обещал разобраться с *Живым журналом*. *Балтийское информационное агентство Balt.Info*. 2011. 20 августа. http://www.baltinfo.ru/2011/08/20/Premer–Kazakhstana–obeschal–razobratsya-s-Zhivym-zhurnalom-223847 (последнее посещение — 26 августа 2012 г.).

[22] Каримов И. А. Концепция дальнейшего углубления демократических реформ и формирования гражданского общества в стране. *Узбекское агентство информации и связи*. 2010. 13 ноября. http://www.aci.uz/ru/news/news/article/2265/(последнее посещение — 27 августа 2012 г.).

[23] Концепции развития информатизации Республики Узбекистан. *Право и СМИ Центральной Азии*. http://medialaw.asia/document/–2718 (последнее посещение — 27 августа 2012 г.).

[24] Доклад о состоянии законодательства о СМИ в Республике Узбекистан. *Право и СМИ в Центральной Азии*. 2008. 13 апреля. http://medialaw.asia/document/–1265 (последнее посещение — 26 августа 2012 г.).

[25] Экономическая основа деятельности средств массовой информации. *Право и СМИ в Центральной Азии*. 2011. 15 мая. http://medialaw.asia/document/1265-1296 (последнее посещение — 26 августа 2012 г.).

[26] См. подробнее:

Закон Республики Узбекистан «О гарантиях и свободе доступа к информации» от 24.04.1997. № 400 — I. *Ведомости Олий Мажлиса Республики Узбекистан*. Ташкент. 2001. № 1–2. С. 23.

Закон Республики Узбекистан «О защите государственных секретов» от 07.05.1993. *Ведомости Верховного Совета Республики Узбекистан*. Ташкент. 1993. № 5. С. 232.

Закон Республики Узбекистан «О защите профессиональной деятельности журналистов» от 24 апреля 1997 г. № 402–I. *Ведомости Олий Мажлиса Республики Узбекистан*. — Ташкент, 1997. — № 4–5. — С. 110.

Закон Республики Узбекистан «О рекламе» от 25.12.1998. № 723–I. Собрание законодательства Республики Узбекистан. Ташкент. 2010. № 37. С. 317.

Закон Республики Узбекистан «О средствах массовой информации» от 26.12.1997. № 541–I (в редакции Закона РУз от 15 января 2007 г. — № ЗРУз–78). Собрание законодательства Республики Узбекистан. Ташкент. 2007. № 3. С. 20.

Закон Республики Узбекистан «Об авторских и смежных правах» от 20.07.2006. № ЗРУ–42. Собрание законодательства Республики Узбекистан. Ташкент. 2006. № 28–29. С. 260.

Закон Республики Узбекистан «Об информатизации» от 11.12.2003. *Ведомости Олий Мажлиса Республики Узбекистан*. Ташкент. 2004. № 1–2. С. 10.

[27] Домену UZ исполнилось 16 лет. Газета.uz. 2011. 1 мая. http://www.gazeta.uz/2011/05/01/cctld/(последнее посещение — 27 августа 2012 г.).

[28] Более 80% домохозяйств и более 40% хозяйствующих субъектов, подключенных к интернету, подключаются через модемное соединение, а по технологии xDSL — около 7% домохозяйств и 36% хозяйствующих субъектов.

[29] UZ 16 лет. Info.nic.ru. 2011. 5 мая. http://info.nic.ru/node/3631 (последнее посещение — 27 августа 2012 г.).

[30] В зоне UZ зарегистрировано 14 тысяч доменов. *Газета.uz*. 2012. 27 марта. http://www.gazeta.uz/2012/03/27/uz/(последнее посещение — 27 августа 2012 г.).

[31] Регистрация доменов с целью перепродажи по более высокой цене во многих национальных законодательствах, включая РФ, не является противоправным действием и не регулируется.

[32] Домену UZ исполнилось 16 лет. *Газета.uz.* 2011. 1 мая. http://www.gazeta.uz/2011/05/01/cctld/(последнее посещение — 27 августа 2012 г.).

[33] Принята программа развития ИКТ на 2012–2014 гг. *Газета.uz*. 2012. 28 марта. http://www.gazeta.uz/2012/03/28/ict/(последнее посещение — 27 августа 2012 г.).

[34] Исмоилов С. Египетский синдром в реалиях Узбекистана. Общество прав человека Узбекистана. 2011. 22 февраля. http://ru.hrsu.org/archives/1793 (последнее посещение — 27 августа 2012 г.).

[35] *Етар*! [*Хватит*!] — молодежное движение, созданное гражданами Узбекистана в 2005 г. Деятельность организации в основном осуществляется в интернете. *Етар*! — название, девиз и призыв молодежного движения, за которым, по словам его представителей, стоят 25–30 молодых людей, граждан Узбекистана. Своей целью движение провозглашает мирное отстранение от власти президента Ислама Каримова, который, по их убеждению, исчерпал два президентских срока управления страной (в 2007 г.), определенных Конституцией республики, и в настоящее время находится во главе Узбекистана незаконно.

[36] Исламу Каримову хотят сказать «Етар!». Независимая информационная служба Узбекистана Uznews.net. 2011. 11 апреля. http://www.uznews.net/news_single.php?lng=ru&cid=30&sub=&nid= 16892 (последнее посещение — 27 августа 2012 г.).

[37] Троллинг (от англ. trolling — ловля на блесну) — размещение в Интернете (на форумах, в дискуссионных группах, ЖЖ и др.) провокационных сообщений, чтобы вызвать конфликты между субъектами, взаимные оскорбления и т. п.

[38] Законодательство в области СМИ Кыргызстана. *Право и СМИ в Центральной Азии*. 2011. 6 января. http://www.medialawca.org/legislation/37/21 (последнее посещение — 26 августа 2012 г.).

[39] В Кыргызстане количество абонентов сотовой связи составило 98% от общего числа населения страны. *Газета Жэньминь Жибао онлайн*. 2011. 2 июня. http://russian.people.com.cn/31519/7398078.html (последнее посещение — 27 августа 2012 г.).

[40] Темир Сариев объяснил, почему *Кыргызтелеком* выставлен на продажу. *K–News*. 2012. 27 марта. http://www.knews.kg/ru/parlament_chro/13338/(последнее посещение — 26 августа 2012 г.).

[41] Регламент на услуги по регистрации доменов в зоне.KG. Kyrgyzstan Domain Registration Service. 2010. 2 декабря. http://www.domain.kg/rus/regulation.htm (последнее посещение — 26 августа 2012 г.).

[42] Президент Кыргызстана обиделся? Host: О хостинге и доменах. 2009, 14 апреля, http://ohost.ru/blog/topic/1043/(последнее посещение — 27 августа 2012 г.).

[43] Законодательство о СМИ стран Центральной Азии (Туркменистан). *Право и СМИ в Центральной Азии*. 2011, 6 января, http://medialaw.asia/legislation/39/21 (последнее посещение — 27 августа 2012 г.).

[44] Законодательство в области СМИ Туркменистана. *Право и СМИ Центральной Азии*. 2011, 6 января, http://www.medialawca.org/analysis/39/21 (последнее посещение — 27 августа 2012 г.).

[45] Туркмения. *Info.nic.ru.* 2011, 5 мая, http://info.nic.ru/node/2736 (последнее посещение — 27 августа 2012 г.).

[46] В национальном домене Туркмении открыта свободная регистрация. Info.nic.ru. 2003, 14 марта, http://info.nic.ru/st/25/out_349.shtml (последнее посещение — 27 августа 2012 г.).

[47] Интернет в стране абсурда. *Туркменский Хельсинкский фонд*. 2008, 12 декабря, http://www.tmhelsinki.org/ru/modules/news/article.php?storyid=1075 (последнее посещение — 27 августа 2012 г.).

[48] Туркменистан. Враг Интернета. Reporters without Borders for Press Freedom. 2011, 4 апреля, http://en.rsf.org/IMG/pdf/turkmenistan_ru–2.pdf (последнее посещение — 27 августа 2012 г.).

[49] Екатеринбургская декларация глав государств — членов Шанхайской организации сотрудничества (последнее посещение — 26 августа 2012 г.).

[50] Декларация десятого заседания Совета глав государств — членов Шанхайской организации сотрудничества. Информационный портал ШОС. 2010, 11 июня, http://www.infoshos.ru/ru/?id=74 (последнее посещение — 26 августа 2012 г.).

[51] Цивилизационная идеология для ШОС. Информационная цивилизация. XXI век. http://www.info21.ru/second.php?id=108 (последнее посещение — 26 августа 2012 г.).

[52] Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 г. на имя Генерального секретаря. A/66/359. Генеральная Ассамблея. Организация Объединенных Наций. 2011. 14 октября. http://rus.rusemb.org.uk/data/doc/internationalcoderus.pdf (последнее посещение — 26 августа 2012 г.).

[53] Там же.

[54] Подробнее о Правилах поведения в области обеспечения международной информационной безопасности см. статью в настоящем номере *Индекса Безопасности*: Демидов О. Обеспечение международной информационной безопасности и российские национальные интересы. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 122.

[55] Решение Совета коллективной безопасности Организации Договора о коллективной безопасности «О программе совместных действий по формированию системы». 2008, 5 сентября, http://www.info21.ru/second.php?id=108 (последнее посещение — 26 августа 2012 г.).

[56] ПРОКСИ — сокращение от «противодействие криминалу в сфере информации». Эта операция — составная часть программы по формированию системы информационной безопасности государств — членов ОДКБ.

[57] ОДКБ проводит операцию против киберпреступности. *РИА-Новости*. 2010, 18 марта, http://ria.ru/defense_safety/20100318/215077305.html (последнее посещение — 26 августа 2012 г.).

[58] Главы ООН и ОДКБ подпишут в четверг заявление о сотрудничестве. *РИА-Новости*. 2010. 18 марта. http://docs.pravo.ru/document/view/16658488/?mode=full (последнее посещение — 26 августа 2012 г.).

Олег Демидов

ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РОССИЙСКИЕ НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ

За последние два года вопросы, связанные с информационным пространством, окончательно перешли в разряд высших приоритетов международной безопасности. Свидетельствами этого стали сразу несколько событий и процессов, которые выглядят дистанцированными друг от друга, но уходят корнями в одну и ту же проблематику.

Во-первых, революционные события так называемой *Арабской весны* в мировом экспертном, медийном и политическом дискурсе оказались неразрывно связаны с ролью информационно-коммуникационных технологий (ИКТ). Несмотря на обильную спекулятивную составляющую и склонность преувеличивать роль социальных сетей и других инструментов Web 2.0 в революционных событиях на Ближнем Востоке и за его пределами, этот дискурс не был полностью лишен оснований. Беспрецедентная скорость распространения информации через интернет (в основном через социальные сети) сыграла против режимов, стремившихся скрыть свои репрессивные акции от международного сообщества и не владевших адекватными навыками ведения информационной борьбы. В то же время обилие непроверенной информации и попытки манипулирования ей привели к искажению глобальной информационной картины событий, которые происходили в Ливии, Сирии и других государствах Ближнего Востока.

Во-вторых, в США были приняты сразу два весьма значимых доктринальных документа, затрагивающих проблематику безопасности киберпространства. Международная стратегия по действиям в киберпространстве была опубликована 16 мая 2011 г. Ее логическим развитием в военной плоскости стала Стратегия Министерства обороны по действиям в киберпространстве, частично рассекреченная и опубликованная в июне 2011 г. В обоих документах киберпространство признается *средой действий*, то есть пространством проведения операций американских вооруженных сил наряду с землей, морем, воздухом и космосом[1]. Безопасность киберпространства впервые оказалась де-факто приравнена по своему значению к военной безопасности — и сделала это единственная в мире военная сверхдержава.

Последним по хронологии, но не по значимости событием в этом ряду стали инициативы России и представителей Шанхайской организации сотрудничества (ШОС), направленные на формирование глобального режима обеспечения безопасности информационного пространства. Речь идет прежде всего о концепции Конвенции ООН «Об обеспечении международной информационной безопасности». Концепция была презентована международному сообществу в ноябре 2011 г. на конференции по киберпространству в Лондоне. Чуть менее резонансной, но столь же масштабной по своим целям инициативой стал проект Правил поведения в области обеспечения международной информационной безопасности, направлен-

ный Генеральному секретарю ООН 12 сентября 2011 г. письмом от четырех государств — членов ШОС.

Наибольший интерес с международно-политической точки зрения вызывает концепция Конвенции об обеспечении МИБ. Представленный проект документа обладает несколькими характеристиками, которые позволяют назвать его не имеющим аналогов в международно-правовой практике регулирования информационного пространства. Так, в числе прочего проект документа:

- претендует на всеобъемлющий характер и полное урегулирование проблематики МИБ;
- должен через механизм ООН получить глобальный охват, распространившись на все международное сообщество;
- предполагает юридически обязывающий характер, не ограничиваясь декларативными заявлениями и формулированием общих принципов поведения государств в информационном пространстве;
- позиционируется как почти завершенный механизм, который, с точки зрения его авторов и сторонников, после соответствующей доработки может превратиться в действующий международно-правовой инструмент ООН уже в ближайшие годы.

С учетом этого российская инициатива в случае ее реализации станет значимой новацией для международного права в сфере ИКТ. Кроме того, превращение российских инициатив в механизмы ООН также будет иметь глобальные политические и военно-стратегические последствия. Поэтому концепция Конвенции, а также проект Правил поведения в области обеспечения МИБ (пусть и меньшей степени) напрямую затрагивают не только национальные интересы РФ, но и интересы ее ключевых зарубежных партнеров.

В связи с этим в настоящей статье инициативы Москвы и ее партнеров по ШОС в области обеспечения МИБ рассматриваются одновременно под углом российских национальных интересов и в то же время приоритетов мирового сообщества и его отдельных представителей, чьи позиции создают преграду продвижению российских проектов.

В рамках статьи предполагается осветить следующие вопросы:

1. Насколько недавние инициативы РФ и ее партнеров отвечают национальным российским интересам и интересам наших зарубежных партнеров и имеют шансы на реализацию в изначально задуманном формате?
2. Как рассматриваемые инициативы отразятся на политике России в области международного сотрудничества по борьбе с киберпреступностью? Необходимо ли России присоединяться к существующим механизмам в этой области или предлагать международному сообществу собственные решения, и какими они могут быть?
3. Какие меры может предпринять российское руководство для того, чтобы сблизить подходы и преодолеть наиболее острые противоречия с зарубежными партнерами и перевести строительство международного режима обеспечения МИБ из сферы дискуссий в практическое русло на компромиссной основе, но не отказываясь при этом от своих инициатив и их основополагающих принципов?

В *Таблице 1* представлены некоторые документы, затрагивающие вопросы обеспечения МИБ, включая действующие механизмы международного права (Екатеринбургское соглашение ШОС от 16 июня 2009 г.) и неофициальные проекты международно-правовых актов. К числу последних относится проект Глобального договора о кибербезопасности и киберпреступности авторства норвежского киберюриста Штайна Шольберга. В приведенной таблице все инициативы, включая

правительственные и неофициальные, упорядочены в рамках простейшей классификации по двум критериям:

а) уровень регулирования (от национального до глобального);

б) направления угроз, противодействие которым является приоритетом для того или иного документа.

Таблица 1. **Соотношение ключевых нормативно-правовых актов по сферам и уровням регулирования информационной безопасности**

Тип угроз/уровень регулирования	Кибер-преступность (*Citizens vs. Citizens*)	Кибер-шпионаж	Агрессивные действия государств в информационном пространстве		Информационный терроризм (*Citizens vs. States*)
			против государств (*States vs. Citizens*)	против граждан (*States vs. States*)	
Глобальный	КОНВЕНЦИЯ О МИБ ДОГОВОР ШОЛЬБЕРГА КОНВЕНЦИЯ СЕ ПРАВИЛА ПОВЕДЕНИЯ (ШОС)	КОНВЕНЦИЯ О МИБ ДОГОВОР ШОЛЬБЕРГА ПРАВИЛА ПОВЕДЕНИЯ (ШОС)	КОНВЕНЦИЯ О МИБ ДОГОВОР ШОЛЬБЕРГА (только кибер-пространство) ПРАВИЛА ПОВЕДЕНИЯ (ШОС)	?	КОНВЕНЦИЯ О МИБ ДОГОВОР ШОЛЬБЕРГА (только кибер-терроризм) ПРАВИЛА ПОВЕДЕНИЯ (ШОС)
Регио-нальный	СОГЛАШЕНИЕ ШОС 2009 КОНВЕНЦИЯ СЕ	СОГЛАШЕНИЕ ШОС 2009	СОГЛАШЕНИЕ ШОС 2009		СОГЛАШЕНИЕ ШОС 2009
Нацио-нальный	НАЦИОНАЛЬНАЯ СТРАТЕГИЯ КИБЕР-/ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ				

Условные обозначения:
КОНВЕНЦИЯ О МИБ — российская концепция Конвенции об обеспечении международной информационной безопасности ООН, презентованная в ноябре 2011 г.
ДОГОВОР ШОЛЬБЕРГА — неофициальный проект Глобального договора о кибербезопасности и киберпреступности ООН Штайна Шольберга и Соланж Гернутти-Эли.
ПРАВИЛА ПОВЕДЕНИЯ (ШОС) — проект Правил поведения государств в области обеспечения международной информационной безопасности, выдвинутый странами — членами ШОС, включая Россию, в сентябре 2011 г.
СОГЛАШЕНИЕ ШОС 2009 — Межправительственное соглашение государств — членов ШОС о сотрудничестве в области обеспечения МИБ от 16 июня 2009 г.
КОНВЕНЦИЯ СЕ — Конвенция Совета Европы «О киберпреступности», открытая для подписания 23 ноября 2001 г.

Кроме того, в таблице фигурирует национальная стратегия информационной безопасности (или, как альтернатива, стратегия кибербезопасности), которая замыкает на себя вопросы обеспечения безопасности в области использования ИКТ как часть национальной государственной политики. Вопрос о том, нуждается ли Россия в выработке и принятии подобной стратегии, призванной дополнить и раз-

вить существующую Доктрину информационной безопасности от 2000 г., является дискуссионным и требует отдельного исследования, выходящего за рамки данной статьи. Также за рамки настоящей работы вынесен вопрос относительно того, какими механизмами должно регулироваться противодействие агрессивному поведению в киберпространстве государств и действующих в их интересах посредников в отношении частного сектора, гражданского общества и отдельных пользователей. Пока эта проблема остается нерешенной как на национальном, так и на международном уровнях.

ИСТОРИЯ РОССИЙСКИХ ИНИЦИАТИВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МИБ И МЕЖДУНАРОДНАЯ РЕАКЦИЯ НА НИХ

РФ в течение долгого времени уделяла значительное внимание продвижению тематики международного взаимодействия в сфере обеспечения МИБ через каналы ООН. Подробный обзор участия Российской Федерации в выработке механизмов регулирования безопасности информационного пространства приводит в своих работах и выступлениях А. В. Крутских. С весны 2012 г. г-н Крутских занимает должность специального координатора по вопросам использования ИКТ в политических целях в МИД России[2]. Начиная с первой половины *нулевых* годов именно он возглавлял российские делегации и группы правительственных экспертов ООН, которые создавались в рамках инициатив по изучению возможностей международного сотрудничества для борьбы с угрозами МИБ.

Как отмечает г-н Крутских, «с 1998 г. Россия продвигает идею налаживания международного сотрудничества по укреплению МИБ», при этом с самого начала «работа по согласованию конкретных мер в интересах упрочения МИБ проводилась главным образом через механизм ООН»[3]. Действительно, ежегодно в течение ряда лет российской стороной на рассмотрение Генассамблеи ООН вносились проекты резолюций «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». В проектах резолюций содержались призывы к рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, а также возможных мер по ограничению угроз, возникающих в этой сфере.

Первая из этих резолюций (A/RES/53/70) от 4 декабря 1998 г. была принята Генеральной Ассамблей без голосования, консенсусом[4]. Однако принятый текст резолюции не соответствовал изначальному варианту, который был направлен Генеральному Секретарю ООН в письме от 23 сентября 1998 г. от постоянного представителя РФ при ООН, российского министра иностранных дел И. С. Иванова. Уже на тот момент в приложенном к письму проекте резолюции были сформулированы ключевые цели, которые отечественная дипломатия пытается решить сегодня в рамках концепции Конвенции об обеспечении МИБ. В частности, в проекте резолюции всем государствам — членам ООН предлагалось информировать Генерального Секретаря о своих взглядах на:

- использование информационных технологий в военных целях;
- определение понятий «информационное оружие» и «информационная война»;
- целесообразность строительства международно-правовых режимов с целью запрещения разработки особо опасных форм информационного оружия[5].

Однако в итоговом варианте резолюции эти проблемы не были отражены. Несмотря на это, вносимые Российской Федерацией резолюции принимались Генеральной Ассамблеей консенсусом в последующие годы, вплоть до 2005 г.

Еще одним направлением, на котором российская дипломатия активизировала свои усилия для обсуждения вопросов обеспечения МИБ, стало двустороннее

российско-американское обсуждение этой проблематики, также начатое в 1998 г. Итогом такого обсуждения стало *Совместное российско-американское заявление об общих вызовах безопасности на рубеже XXI в.*, которое президенты РФ и США подписали 2 сентября 1998 г. На том этапе, однако, существенных успехов в плане продвижения своего понимания МИБ российской стороне добиться не удалось. В тексте совместного заявления «ослабление действия негативных аспектов информационной технологии» признавалось «серьезной задачей в деле обеспечения стратегических интересов безопасности наших двух стран в будущем»[6]. Однако никакой системы международного сотрудничества документ не предлагал, а в части конкретики уделял внимание взаимодействию по совместному преодолению актуальной на тот момент «проблемы–2000», связанной со сменой компьютерных кодировок с наступлением новой календарной даты. Вместе с тем сам факт появления совместного заявления стал существенным шагом для двух стран в плане признания проблематики МИБ как важной составляющей двусторонних отношений. Кроме того, практика двустороннего российско-американского взаимодействия и совместных заявлений получила развитие в дальнейшем, спустя многие годы. 28 июня 2011 г. было опубликовано совместное заявление заместителя секретаря Совета Безопасности Российской Федерации Н. В. Климашина и (на тот момент) координатора Белого дома по кибербезопасности Говарда Шмидта.

Помимо двусторонних обсуждений и внесения проектов резолюций на сессиях Генассамблеи ООН Российская Федерация активно использовала механизм Групп правительственных экспертов (ГПЭ) ООН для продвижения повестки дня в области МИБ. Впервые ГПЭ ООН была учреждена 8 декабря 2003 г. во исполнение резолюции ГА ООН A/RES/56/19 от 29 ноября 2001 г. Целью Группы была активизация международного рассмотрения существующих и потенциальных угроз в сфере информационной безопасности, возможных мер по ограничению таких угроз, возникающих в этой сфере, и изучение международных стратегий, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем[7]. Первый проект доклада по итогам работы Группы был подготовлен в 2004 г., однако в изначальном виде не был принят консенсусом из-за серьезных разногласий между членами Группы и, в частности, противодействия российскому подходу со стороны представителей США. В результате в 2005 г. удалось принять лишь процедурный доклад A/60/202, в котором констатировалось, что «с учетом сложного характера вопросов, о которых идет речь, не было достигнуто консенсуса относительно подготовки окончательного доклада»[8].

Противоречия между участниками ГПЭ касались прежде всего двух вопросов, имевших политическое значение. Первый из них, принципиально важный для представителей РФ, касался военно-политических аспектов ИКТ и влияния этих технологий на национальную безопасность и международный военно-политический баланс. Несмотря на общее признание важности этих вопросов членами ГПЭ, им не удалось прийти к общему мнению относительно того, стоит ли включать в текст доклада формулировки, которые смещали бы общий акцент на угрозы, обусловленные использованием ИКТ в военно-политических целях государствами. Второе противоречие касалось вопроса о том, должны ли быть предметом рассмотрения Группы вопросы, связанные с содержательным наполнением распространяемой информации — *контентом*, или рассматривать следует лишь те вопросы, которые связаны с безопасностью информационной инфраструктуры. Первую точку зрения можно с некоторыми оговорками назвать *российской*, вторую — *американской*. Один из конкретных вопросов в этой связи касался того, следует ли рассматривать передачу и распространение трансграничной информации через ИКТ-сети в качестве вопроса национальной безопасности и обеспечивать соответствующий контроль над ними[9].

Призыв к созданию следующей ГПЭ прозвучал, вновь по инициативе России, уже 8 декабря 2005 г., когда была принята очередная резолюция «Достижения в сфере информатизации...» (A/RES/60/45)[10]. Как отмечает А. В. Крутских, возглавивший вторую ГПЭ, «несмотря на давление американской делегации [...] россий-

ские предложения по вопросам МИБ поддержали Япония, Израиль, Южная Корея, Австралия и Канада»[11]. Группа из 15 экспертов–представителей различных стран была сформирована в 2009 г. и завершила свою деятельность в 2010 г. после серии из четырех сессий. В отличие от предыдущей ГПЭ, итогом работы второй Группы стал принятый консенсусом и представленный на 65-й сессии Генеральной ассамблеи в июле 2010 г. доклад, который отразил некоторые ключевые вопросы и озабоченности российской стороны по поводу применения ИКТ в военно-политических целях. В частности, в докладе отмечается, что ИКТ могут «использоваться в целях создания угрозы международному миру и национальной безопасности». Кроме того, впервые в рамках ООН в документе была прямо отмечена угроза, связанная с тем, что «государства разрабатывают ИКТ в качестве инструментов ведения войны и разведки и для применения в политических целях». Наконец, в число итоговых рекомендаций в докладе было включено «принятие мер по укреплению доверия, обеспечению стабильности и уменьшению рисков в связи с последствиями государственного использования ИКТ, включая обмен мнениями стран по вопросу об использовании ИКТ в конфликтах»[12]. С учетом таких формулировок деятельность второй ГПЭ стала *прорывом* для России, сумевшей существенно продвинуть повестку дня в сфере ИКТ с учетом тех аспектов, которые являлись — и до сих пор являются — для нее центральными.

Последняя, третья ГПЭ была учреждена резолюцией Генассамблеи ООН A/RES/66/24, принятой без голосования 2 декабря 2011 г., чтобы продолжить изучение существующих и потенциальных угроз в сфере информационной безопасности, а также возможных стратегий по рассмотрению таких угроз. Деятельность группы, в которую, как и в предыдущие ГПЭ, входят российские представители, включает три встречи недельной продолжительности. Первая из встреч Группы прошла 6–10 августа 2012 г. в Нью-Йорке, последняя состоится там же в июне 2013 г.

В общем и целом деятельность ГПЭ внесла большой вклад в продвижение проблематики ИКТ в контексте МИБ, и в том числе российского видения этих вопросов. Любопытно, что с течением времени даже США перестали отрицать важность проблемы использования ИКТ государствами в военно-политических целях. В докладе Генерального секретаря ООН от 15 июля 2011 г. (A/66/152) в ответе, полученном от правительства США, среди мотивов деятельности, создающей угрозы работе глобальной сети и критических инфраструктур, упоминается «перенесение традиционных форм государственного конфликта в киберпространство»[13], а в число субъектов, создающих такие угрозы, включены государства. В том же докладе отмечается, что «в ряде обстоятельств подрывная деятельность в киберпространстве может представлять собой вооруженное нападение»[14]. Вместе с тем Вашингтон по-прежнему отстаивает приоритет вопросов инфраструктуры и не желает рассматривать проблему содержания трансграничных информационных потоков в плоскости международной безопасности.

Кроме того, в контексте настоящей статьи немаловажно то, что дискуссии в ходе деятельности ГПЭ и обсуждения проектов вышеназванных резолюций позволили выработать некий вариант *нейтральной терминологии*. В тексте резолюций рассматриваемая проблематика формулируется вне рамок западной лексики кибербезопасности и, по большей части, не в терминах «обеспечения МИБ». Поиски участниками ГПЭ взаимоприемлемых формулировок с целью нахождения компромисса привели к тому, что тексты резолюций обращены к проблематике «ИКТ в контексте международной безопасности», что корректно и нейтрально, хотя и достаточно размыто, характеризует суть затрагиваемых вопросов. Потенциал использования официальной терминологии резолюций Генассамблеи ООН для сближения подходов РФ и ее зарубежных партнеров в настоящее время будет рассматриваться ниже.

Сегодня можно говорить о том что, несмотря на впечатляющую активность России в продвижении проблематики обеспечения МИБ за последние 15 лет, с разработкой концепции Конвенции в 2011 г. усилия российской дипломатии вышли

на принципиально новый уровень. Полноценная презентация документа прошла 1 ноября 2011 г. в Лондоне, на Конференции по вопросам киберпространства. С речью, посвященной преимущественно концепции Конвенции, выступил И. О. Щеголев, на тот момент глава Министерства связи и массовых коммуникаций РФ. Незадолго до этого, 22 сентября 2011 г. документ был представлен главам спецслужб и силовых ведомств 52 стран на встрече в Екатеринбурге[15]. Чуть ранее, 12 сентября 2011 г. Генеральному секретарю ООН было направлено письмо от Постоянных Представителей в ООН четырех государств ШОС — России, Китая, Узбекистана и Таджикистана. К письму прилагался проект Правил поведения в области обеспечения международной информационной безопасности. В отличие от концепции Конвенции, Правила не носят юридически обязывающего характера, но в целом воспроизводят проблематику концепции Конвенции, хотя и без столь явного упора на военно-политическую составляющую информационной безопасности.

Международная реакция на инициативы Москвы в большинстве случаев характеризуется довольно острым интересом, который, однако, до настоящего времени не выливался в конкретные встречные инициативы. В Азиатско-Тихоокеанском регионе, где Россия пыталась последовательно наращивать активность в преддверии Саммита АТЭС в августе 2012 г., идеи Конвенции и Правил поведения были встречены противоречиво. В рамках Азиатско-Тихоокеанского совета сотрудничества по безопасности (АТССБ), *трека два*, объединяющего 22 страны региона, включая Индию, США, Японию, Китай и Россию, инициативы РФ и ШОС были встречены с интересом, но также с недоверием и определенным скепсисом. Наибольший интерес к ним проявляет Индия, претендующая на роль одной из ведущих IT-держав и в то же время все более опасающаяся киберугроз, исходящих от Китая, своего основного соперника в Азии. В апреле 2012 г., в Гармиш-Партенкирхене (ФРГ) прошел шестой международный форум[16], посвященный в основном вопросам МИБ. В ходе форума впервые публично обсуждалась российская концепция Конвенции. В поддержку документа высказался заместитель главы организации оборонных исследований Минобороны Индии Амит Шарма, призвав дополнить российский проект определениями из области кибербезопасности, в частности понятиями *национального киберпространства* и *враждебных действий государств в киберпространстве*. В целом, в восточноазиатском регионе для России в плане обсуждения вопросов международной безопасности интересны прежде всего Восточно-Азиатские саммиты, АСЕАН и Региональный форум АСЕАН — АРФ, а также упомянутый *трек* АТССБ. На данный момент, спустя год после презентации концепции Конвенции, в рамках этих форматов не было принято конкретных решений о поддержке российских инициатив. Однако привлечение на сторону российского подхода Индии представляется весьма важной задачей. Россия вместе с КНР — лишь две крупные державы, отстаивающие собственное понимание роли ИКТ в контексте международной безопасности. С Индией речь идет уже о половине человечества, включая «крупнейшую в мире демократию».

Одна из ключевых причин осторожного отношения к российским инициативам состоит в том, что проблематика военно-политического использования ИКТ по-прежнему остается чувствительной для ряда государств и не всегда включается в повестку дня многостороннего международного взаимодействия. К примеру, на встрече Рабочей группы по кибербезопасности АТССБ в Бенгалуру в октябре 2011 г. реакция на инициативу эксперта ПИР-Центра о внесении в повестку дня вопросов агрессивного поведения государств в киберпространстве сводилась к тезису о том, что этот вопрос не укладывается в формат деятельности группы. При этом — и такой подход характерен отнюдь не только для формата АТССБ — вопрос военно-политических аспектов применения ИКТ позиционируется как фактор, который политизирует повестку дня и подразумевает необходимость «дружбы против третьего». Подобное понимание сути и цели проблем, которые поднимает российская сторона, довольно далеко от действительности. Однако его широкое распространение говорит, в том числе, о том, что сама концепция Конвенции

и родственные ей инициативы в нынешнем виде звучат недостаточно внятно и четко и оставляют пространство для интерпретации их задач и приоритетов.

Кроме того, для части российских партнеров, прежде всего для ЕС и США, объектом критики выступают нормы концепции Конвенции, предполагающие запрет на распространение информации, «которая вдохновляет терроризм, сепаратизм, экстремизм или подрывает политическую, экономическую и социальную стабильность других стран». В данных положениях зарубежные партнеры РФ усматривают скрытый потенциал для интернет-цензуры и контроля над национальными сегментами глобальной Сети. Так, после ноябрьской конференции 2011 г. в Лондоне заместитель госсекретаря США Майкл Познер назвал проект Правил поведения в области обеспечения МИБ неприемлемым решением, за счет которого интернет превращается «из пространства, управляемого множеством людей и заинтересованных сторон», в систему, «подконтрольную центральным правительствам»[17]. С момента презентации концепции Конвенции и Правил поведения целый ряд аналогичных заявлений был озвучен высокопоставленными чиновниками и дипломатами США, СЕ и стран Европы. Тональность высказываний западных дипломатов не претерпела существенных изменений и год спустя, на очередной конференции по вопросам киберпространства в Будапеште 4–5 октября 2012 г. Как заявил в своем выступлении на конференции глава британского МИД Уильям Хейг, прозрачно намекая на российскую концепцию Конвенции, Лондон «не призывает к новому межправительственному договору [по вопросам кибербезопасности], который был бы обременителен в плане согласования, трудновыполним и слишком узок по своему охвату»[18].

При анализе критической реакции зарубежных партнеров России на инициативы в области МИБ следует прежде всего учитывать то, что на Западе и в ряде других стран распространен фундаментально иной подход к вопросам регулирования информационного обмена. Этот подход предполагает принципиально меньший по сравнению с российскими инициативами объем контроля государства над информационными потоками и их содержанием, в том числе применительно к трансграничному информационному обмену. В результате многие вопросы и проблемы, которые затрагивают концепция Конвенции и Правила поведения, наши партнеры вообще не считают уместными для обсуждения и регулирования в категориях международного права.

Подобная точка зрения распространяется на экспансию и доминирование в глобальном информационном пространстве, принуждение государств к принятию решений в чужих интересах и ряд подобных им угроз, которые упоминаются в концепции Конвенции. Прежде всего существование ряда угроз из этого перечня вообще не всегда признается нашими партнерами. Кроме того, большинство акторов, обеспечивающих формирование *контента* в глобальном информационном пространстве, в западных странах не находятся под прямым государственным контролем и зачастую имеют транснациональную природу. Подчинение их нормам межправительственного соглашения, по мнению наших партнеров, не соотносится с логикой *децентрализованного* информационного пространства. Наконец, те виды деятельности (психологическая война), наличие и важность которых не оспариваются, являются приоритетом спецслужб и не подлежат согласованию в рамках международного диалога.

В свою очередь, в основе подхода, который сегодня является концептуальной альтернативой российским инициативам в области обеспечения МИБ, лежит иное определение сферы рассматриваемых проблем и угроз безопасности — через понятие *кибербезопасности*. Соответственно, рассматривается и совсем другая среда — *киберпространство* вместо информационного пространства. Подробный анализ западного подхода выходит за рамки задач настоящей статьи, но в целом необходимо отметить, что парадигматика кибербезопасности включает прежде всего упор на безопасность инфраструктуры компьютерных сетей. Вопросы влияния информационных потоков на социополитические и иные процессы в проблематику кибербезопасности практически не включаются — и это один из основных

идейных разломов с концепцией МИБ. Проблематика кибербезопасности ограничивается спектром цифровых технологий, в отличие от МИБ. В основном границы проблематики кибербезопасности определяются через совокупность информационных систем, функционирующих на основе *двоичного кода*.

Для согласования подходов России и западных государств и лучшего понимания парадигматики кибербезопасности был даже выработан специальный глоссарий с переводом ключевых терминов западного происхождения. В совместном исследовании Института Запад–Восток (East–West Institute) и Института проблем информационной безопасности (ИПИБ) МГУ имени М. В. Ломоносова («*Российско-американский базовый перечень критических понятий в области кибербезопасности*») выработана согласованная русско-английская понятийная база по ключевым военно-политическим вопросам кибербезопасности. В итоговый доклад были включены определения основных 20 терминов, включая кибервойны, киберконфликты и собственно киберпространство[19]. Однако на текущий момент лучшее понимание не способствует сближению двух подходов. Напротив, конкуренция России и ее союзников (КНР и другие государства ШОС) с западными государствами в части утверждения на глобальном уровне того или иного понимания роли ИКТ в контексте международной безопасности приобретает черты идеологического противостояния.

Так или иначе, сущностное рассмотрение концепции Конвенции невозможно без более подробного анализа терминологии, на которой она основана и которая несет в себе принципиальные черты российского подхода к вопросам МИБ, глубоко отличающегося от западных концепций.

ТЕРМИНОЛОГИЯ РОССИЙСКИХ ИНИЦИАТИВ: КОНЦЕПТУАЛЬНЫЕ ВЫЗОВЫ И УЯЗВИМЫЕ МЕСТА

Первой ключевой характеристикой, в равной степени присущей проекту Правил поведения, концепции Конвенции и Екатеринбургскому соглашению ШОС, является опора на понятия информационной безопасности и информационного пространства, которые используются почти в той же форме, в которой они существуют в национальном законодательстве РФ. Ведущая роль российской стороны как теоретика и идеолога названных международных документов и инициатив обусловила тот факт, что именно российский подход лег в основу их терминологической базы. В результате бо́льшая часть понятий и определений, в частности в концепции Конвенции, преемственны либо близко родственны по отношению к российским доктринальным документам.

Однако концептуальные и терминологические противоречия возникают в тех случаях, когда Россия пытается предложить новые для международного права определения, особенно в части регулирования поведения государств в информационном пространстве. Одним из примеров является определение *информационной войны*, которое представляет собой одно из ключевых понятий в рамках российского подхода к обеспечению МИБ. В концепции Конвенции это определение также заимствовано. В рамках законодательства России понятие информационной войны впервые фигурировало в Доктрине ИБ от 2000 г., однако в документе не содержалось соответствующего определения.

С 2009 г. такое определение появилось, причем сразу на уровне действующего международного договора. Понятие и определение информационной войны было зафиксировано в межправительственном соглашении государств — членов ШОС о сотрудничестве в области обеспечения МИБ, которое было подписано 16 июня 2009 г. в Екатеринбурге во время шестого саммита организации (далее по тексту — Екатеринбургское соглашение ШОС). В документе под информационной войной понимается «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва поли-

тической, экономической, социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»[20].

Следует выделить несколько особенностей приведенного определения, которые важны для понимания сути доктринального видения, частью которого оно выступает.

Во-первых, в рамках определения (как и, по большей части, в концепции Конвенции в целом) не упоминается и не рассматривается возможность участия в информационных войнах разного рода *негосударственных акторов*. Между тем государствоцентричное понимание конфликтов в информационном пространстве прямо противоречит реально наблюдаемой картине. Во-первых, если взять в качестве примеров кибератаки в Грузии в 2008 г., в Эстонии в 2007 г., а также атаки на иранские или американские сети в последние годы, за ними всегда стоят некие субъекты, чьи действия могут осуществляться в интересах тех или иных государств, но прямую связь при этом проследить затруднительно или невозможно. Иногда речь действительно идет о лицах и группах, являющихся частью государственных силовых структур и спецслужб. Однако зачастую эти субъекты представляют собой либо группы, действующие автономно из патриотических или иных побуждений, либо *посредников*, которые действуют в интересах и/или по заказу государственных структур, либо иным косвенным образом связаны с ними. Проблема посредников неотделима от вопросов информационных войн, так как одним из ключевых препятствий к использованию механизмов международного права в сфере обеспечения МИБ является нерешенность проблемы атрибуции — определения авторства деструктивных действий в информационном пространстве и ответственности за их осуществление. Как отмечается в исследовании ПИР-Центра, единственным способом, позволяющим достоверно установить связь субъектов, осуществляющих деструктивную деятельность в киберпространстве, с государственными структурами, остается агентурная работа спецслужб. Однако ни одна из национальных разведок в обозримом будущем не будет располагать ресурсами, позволяющими системно решать задачи по выявлению такого рода связи в случае каждой политически мотивированной кибератаки[21].

Другая субстантивная сложность, связанная с определением информационной войны в концепции конвенции и Екатеринбургском соглашении ШОС связана с тем, что оно описывает сразу несколько различных явлений и процессов, между которыми на практике далеко не всегда присутствует взаимосвязь. С одной стороны, под информационной войной фактически понимаются кибератаки на ИКТ-сети и инфраструктуру, с другой же стороны, речь идет о классической *психологической войне* в западном понимании. По этой логике, применение *Stuxnet, Duqu, Flame* и *Gauss* против информационной инфраструктуры в государствах Ближнего Востока, атаки на сервера госучреждений и компаний частного сектора в Эстонии в 2007 г. и в Грузии в 2008 г., а также программы вещания финского телевидения на территорию СССР в 1980-х гг. следует считать эпизодами информационной войны. Вопрос состоит в том, что общего у этих событий и как объединение их в единую категорию угроз помогает выработать дифференцированные подходы к их отражению.

Кроме того, определение информационной войны в концепции Конвенции не совсем корректно идентифицирует цели тех действий и процессов, которые оно в себя включает. В частности, встает вопрос об эффективности определения как рабочего инструмента классификации угроз МИБ применительно к проблеме кибершпионажа, который также может быть составляющей информационной войны. Следует оговориться, что речь не идет о коммерческом кибершпионаже, практикуемом с целью кражи ноу-хау, клиентских баз, карт месторождений и рыночных исследований организаций частного сектора. Ближневосточные сложные вирусы, в частности *Duqu* и *Flame*, являют собой пример кибершпионажа иного уровня и масштаба. Имеется в виду сбор данных о критических объектах, программах,

а также связанных с ними персоналиях, для последующих действий в отношении данных *целевых объектов*. В иранских сетях до сих пор действуют высококлассные инструменты, адаптированные под конкретные учреждения (*Duqu*), а иногда и под конкретных людей, имеющих отношение к ядерной и ракетной программам Тегерана. При этом до последнего времени параллельно функционировало целое семейство программ, по всей вероятности, созданных киберспециалистами из числа американских военных и разведки. На данный момент выявлено, как минимум, четыре беспрецедентно сложных программы (*Stuxnet, Duqu, Flame, Gauss*), не считая серии их модификаций; ведется поиск и других программ (*Wiper*). *Лабораторией Касперского* также выявлены три неиспользованных *заготовки* вирусов с кодом, родственным коду *Flame*[22].

Понятийный аппарат концепции Конвенции не позволяет уверенно ответить на вопрос о том, как квалифицировать подобную деятельность на международном уровне и бороться с ней. Еще одно противоречие здесь заключается в том, что многие эксперты как на Западе, так и в РФ (например, Евгений Касперский[23]) называют *Flame, Gauss, Duqu* и другие шпионские программы, выявленные в иранских сетях, *кибероружием* и характеризуют их применение как эпизод информационной войны. Но в концепции Конвенции об обеспечении МИБ термин «информационное оружие» замкнут на понятие информационной войны и определяется как «информационные технологии, средства и методы», предназначенные для ее ведения. В результате акты кибершпионажа как бы выпадают из понятийного аппарата документа, так как не наносят ущерба информационным системам, критическим структурам и не ведут к психологической обработке населения. Важно подчеркнуть, что *Stuxnet* в данном случае стоит особняком, представляя собой орудие *киберсаботажа*, то есть, несомненно, информационное оружие. А вот как классифицировать *Flame*, который «устанавливает профессиональную систему слежения с четко обозначенными целями»[24], но сам ничему не вредит, из концепции Конвенции неясно.

Представляется, что проект документа должен быть дополнен отдельной статьей, в рамках которой рассматривались бы вопросы кибершпионажа, а также вводилось бы соответствующее определение. Более того, особого пункта и определения *заслуживает кибершпионаж с целью сбора критических знаний и дальнейшего использования в военно-стратегических целях,* который должен рассматриваться не как правонарушение, а как акт международной агрессии. Подобное разделение важно, так как именно подобные программы и средства кибершпионажа сегодня называют кибероружием — без соответствующих юридических оснований.

Спорные моменты в терминологии концепции Конвенции не исчерпываются определением информационной войны. Несколько противоречиво выглядит определение информационного *пространства* как «*сферы деятельности*». Дело в том, что подобная дефиниция затрудняет дальнейшее развитие стратегий и направлений практической деятельности госорганов и иных структур в этой области. Так, во второй половине 2011 г. в Минобороны РФ был подготовлен первый в своем роде документ, который был опубликован в январе 2012 г. под названием *Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве*[25]. Терминология документа полностью идентична понятийному аппарату концепции Конвенции, в том числе в части использования понятия информационного пространства. Однако в этом случае возникает вопрос с частичной рекурсивностью понятия *деятельности ВС в информационном пространстве* — исходя из терминологии обоих документов речь идет о *деятельности в сфере деятельности*. В результате определение не становится некорректным, но страдает размытостью; исходя из него к ведению вооруженных сил должна относиться вся деятельность по формированию, созданию, преобразованию, передаче, использованию, хранению информации. Из этого спектра нельзя выделить задачи, *специфически* присущие вооруженным силам и не присущие СМИ, дипломатии, политическим и негосударственным структурам.

Характерно, что авторы документа Минобороны в результате идут другим путем и определяют деятельность ВС в информационном пространстве как «*использова-*

ние вооруженными силами информационных ресурсов для решения задач обороны и безопасности». Само понятие информационного пространства как отдельного термина из концепции Конвенции и документа Минобороны здесь не используется, а определение формируется на основе другого понятия — информационных ресурсов. Таким образом, нарушается логическая целостность определения и концептуальная стройность документа.

При этом содержание ключевых определений дублируется и воспроизводится в других определениях и статьях документа, в которых содержатся отсылки на них. Так, рассмотренное понятие *информационной войны* в тексте концепции Конвенции фигурирует еще в одном определении и трех статьях. Схожая ситуация наблюдается и с Правилами поведения в области обеспечения МИБ, в которых используется по большей части та же самая терминологическая база.

Специфика подхода к МИБ России и ее единомышленников по ШОС, отраженная в концепции Конвенции, не исчерпывается ее ключевыми определениями. Более принципиальной особенностью документа является видение в национальных государствах ключевых участников глобального информационного обмена, обладающих полным контролем над трансграничными информационными потоками. В рамках этой логики информационное пространство, хотя и является *общечеловеческим достоянием,* тем не менее делится на информационные пространства государств, к которым в полной мере применим принцип государственного суверенитета. Наиболее четко эта идея формулируется в пункте 5 статьи 5 концепции Конвенции, гласящем, что «каждое государство-участник вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством». Суверенитет государства в информационном пространстве подразумевается и пунктом 7 упомянутой статьи, согласно которому «каждое государство-участник имеет право свободно осуществлять без вмешательства извне развитие своего информационного пространства».

Особо важен тот факт, что из подобного подхода напрямую следует государствоцентричность не только информационного пространства, но и самого информационного обмена. Иными словами, подразумевается, что государства в полной мере контролируют *содержание* трансграничных информационных потоков и несут за это содержание ответственность. Такой подход, в частности, постулируется шестым основным принципом обеспечения МИБ концепции Конвенции, который предполагает ответственность государств «за собственное информационное пространство, в том числе за его безопасность и за содержание размещаемой в нем информации». При этом негосударственные участники мирового информационного обмена в документе в основном не упоминаются. В результате логика концепции Конвенции не позволяет документу охватить субъектов, которые в общем-то наполняют мировую систему коммуникаций содержанием и без которых информационный обмен невозможен:

- *Частный сектор.* Организации частного сектора выступают ключевыми субъектами в вопросах, связанных с кибербезопасностью. На частные компании приходится весьма значительная доля кибератак, причем зачастую политически мотивированных. В сетях частных структур ведется основная масса операций кибершпионажа, однако они же выступают абсолютными лидерами в области разработки средств и технологий защиты от киберугроз как рядовых юзеров, так и стратегических компаний и госструктур. Сверхсекретная сеть Пентагона *JWICS (Джейвикс)* не была бы создана без технологий частного сектора; созданием защищенных информационных систем и средств их защиты для российского Минобороны сегодня также занимаются частные компании. В США, КНР, России и других *кибердержавах* ведется активное взаимодействие между военными структурами и сообществами хакеров. Наконец, нельзя обойти тот факт, что частный сектор в лице частных провайдеров, телекоммуникационных корпораций и ИТ-компаний обеспечивает технологическое функционирование и развитие системы глобального обмена информацией. Частный

сектор во многом обеспечивает информационный обмен, предоставление доступа к информации основной массе пользователей, эффективную защиту от угроз в информационном пространстве.

- Отдельного упоминания заслуживают *глобальные СМИ*, которые по большей части также имеют негосударственную природу. От них зависит формирование наполнения, содержания мирового информационного обмена — и они не могут однозначно ассоциироваться с теми или иными государствами. *BBC, CNN, Al Jazeera* зачастую вносят вклад в искажение глобальных информационных потоков — события августа 2008 г. в Грузии, 2011 г. в Ливии, 2012 г. в Сирии и многие другие эпизоды служат тому примерами, но ответственность за их действия не может автоматически возлагаться на Великобританию, США, Катар или любое другое государство. С учетом того, что критерии информации, представляющей угрозу для МИБ, в концепции Конвенции отсутствуют, встает вопрос об имплементации упомянутого принципа ответственности государств за содержание информации в национальных сегментах информационного пространства. Понятия и критерии противозаконной информации существенно варьируются в различных государствах, не говоря уже о том, что львиная доля информации, представляющей угрозы для МИБ в рамках изложенного в концепции Конвенции видения, может вообще не подпадать под правовые санкции в национальных законодательствах. Даже принцип территориальной ответственности государств за *кибер*угрозы, предлагаемый рядом американских экспертов, весьма трудно воплотим на практике, хотя охватывает куда более узкую проблематику. По крайней мере, пока не решена проблема атрибуции в отношении кибератак. Возложение ответственности за действия медиа-акторов на государственные субъекты в рамках принципа территориальной ответственности — тот пункт, который России будет особенно трудно сдвинуть с мертвой точки. Без адекватного юридического обоснования он рискует быть воспринят как норма, подрывающая устои частного сектора и легитимирующая цензуру в СМИ и информационном пространстве в целом. В приведенной формулировке и в отсутствие более подробного ее разъяснения данное положение скорее выглядит контрпродуктивным и рискует вызвать возражения у большинства зарубежных партнеров РФ.

- Не менее важны *интернет-сообщества,* которые играют все большую роль в глобальном информационном обмене в интернете, где отсутствуют иерархия, правовая система, а зачастую и идентификация. Прежде всего существует проблема анонимности, которая делает идею ответственности государств за содержание информационного обмена в Сети достаточно условной. На сегодняшний день в мире не выработаны единые, официально согласованные стандарты и подходы к глобальной интернет-идентификации и аутентификации; простых решений в этой сфере не просматривается[26]. При этом преодоление анонимности участников информационного обмена в Сети сталкивается прежде всего не с техническими проблемами, а с вопросом о том, как быть, если анонимность признается правом? Концепция Конвенции не предлагает решений проблемы анонимности — однако в таком случае принципы, постулируемые в ней, не могут быть эффективно имплементированы. Россия не может нести ответственность за свое информационное пространство, если ее госорганы не имеют права устанавливать личность участников интернет-коммуникаций (пользователей анонимного видеохостинга, чата, блога), пока размещаемая ими информация не нарушает национальное законодательство. При этом тот факт, что информация, создающая угрозу МИБ, автоматически будет носить противоправный характер, далеко не очевиден. Загрузка видео на *YouTube* с недостоверной информацией о событиях в Сирии или Ливии не является правона-

рушением. Однако загрузка сотен тысяч таких видеозаписей в рамках скоординированной кампании — именно то, что положения концепции Конвенции позволяют расценивать как угрозу МИБ.

Помимо проблемы анонимности встает вопрос с трансграничными сервисами, такими как социальные сети. Какое государство должно нести ответственность за мои действия, если в российской сети *ВКонтакте* я, находясь в ФРГ и являясь гражданином США, оставляю на стене пользователя из Польши *перепост* видео пользователя из Украины с призывом к джихаду? И вообще, ответственность лежит на пользователях или на самой социальной сети, допустившей загрузку таких материалов? Вопросы упираются в сетецентричную природу интернета и не имеют легкого и однозначного решения, а в концепции Конвенции этот вопрос и вовсе не рассматривается.

Кроме того, на практике тезис о государствоцентричности информационного пространства оказывается неверен, по крайней мере, для большинства развитых стран, в части государственного контроля над критической информационной инфраструктурой. Не затрагивая тривиальный пример с корневыми серверами системы DNS, которые управляются международной неправительственной и некоммерческой организацией ICANN, мы имеем массу свидетельств подобного рода как в США, где в частной собственности находится до 90% критической инфраструктуры, так и других странах.

В США государство напрямую не контролирует работу информационной системы Нью-йоркской фондовой биржи, капитализация рынка акций которой на ноябрь 2010 г. составляла 13,39 трлн долларов, или около 50% суммарной капитализации мирового фондового рынка[27]. Сама *New York Stock Exchange LLC* по своему правовому статусу близка к российскому понятию общества с ограниченной ответственностью (ООО), что исключает прямой государственный контроль над ее информационной системой. Подтверждением независимого статуса NYSE стали события 11 сентября 2001 г., когда деятельность биржи, расположенной в сравнительной близости от Всемирного торгового центра, оказалась нарушена. Несмотря на то что действия руководства биржи по обеспечению сохранности, безопасности и бесперебойного функционирования ее информационной системы координировались с представителями Комиссии по ценным бумагам и биржам, а также Казначейством США на экстренном совещании, прямого перехвата контроля госорганами не произошло даже в тех чрезвычайных условиях[28, 29].

Важно подчеркнуть, что приведенный пример не может считаться значимым лишь для США уже в силу того, что крупнейшие фондовые биржи являются элементами *глобальной* критической инфраструктуры. Нью-Йоркская биржа обеспечивает стабильность мировой финансовой системы, элементом которой является и финансовая система РФ. То же применимо к информационным системам крупных промышленных объектов, таких как ГЭС, АЭС, газопроводы, трансграничные энергосети, операторами которых в развитых странах чаще всего являются структуры частного сектора. Согласно исследованию компании *Symantec* за октябрь 2010 г., 85% всей критической инфраструктуры США, подключенной к информационным сетям, находится под контролем частных операторов, включая энергетические сети, промышленную, транспортную, финансовую инфраструктуру[30]. В большинстве случаев работу объектов критической инфраструктуры обеспечивают частные информационные сети, атака на которые способна привести к последствиям, далеко выходящим за рамки национальных границ или отдельно взятого региона.

Вообще, делегируя государствам право выступать на мировой арене от имени всех участников глобального информационного обмена, концепция Конвенции рискует столкнуться с проблемой фундаментального характера. Несколько десятилетий назад проблема регулирования деятельности трансграничных акторов рассматривалась в контексте Кодекса ООН для транснациональных корпораций (ТНК). Проект такого кодекса в разных вариантах прорабатывался с 1972 по 1992 г. и в итоге был отклонен, так как делегаты ООН сочли консенсус по его проек-

ту невозможным[31]. За 20 лет работы над Кодексом так и не удалось согласовать правовой механизм, который обеспечивал бы юридически обязывающий характер кодекса, предлагал реальные варианты имплементации прописанных в нем норм и не ущемлял бы интересы самих ТНК. Причина неудачи заключалась в том, что государства сегодня неспособны самостоятельно, без участия других субъектов и посредников регулировать те институты, процессы и явления, которые развиваются преимущественно вне национальных границ и систем нормативно-правового регулирования. А в случае с глобальным информационным пространством процесс преимущественно протекает вообще вне рамок государственного административного контроля.

Установление такого контроля сегодня — весьма сложная задача, особенно в части верификации исполнения тех норм, которые предлагает российская концепция Конвенции. В частности неясно, как обеспечить верификацию в части отказа от создания кибероружия. Возможностями по созданию таких средств сегодня обладает абсолютное большинство государств мира, при том, что такие возможности доступны и негосударственным акторам. По оценке российских дипломатов, эксперименты «в области ведения информационных или кибервойн» сегодня ведут не менее 120 государств[32]. Отследить разработки кибероружия той или иной группой субъектов на ранних этапах до его применения пока практически невозможно, в отличие от ОМУ и космического оружия, — для их создания требуется минимальный объем общедоступной технической инфраструктуры. Несколько упрощая, для этого достаточно ПК и *флэшки.* Что касается средств ведения информационной войны *за рамками* ее кибернетических аспектов, то здесь оружием может выступать каждое СМИ, блог и аккаунт отдельного пользователя Сети.

Названные факторы наряду с трансграничным характером глобальных медиа и минимальным контролем над интернет-пользователями во многих странах мира вызывают серьезные сомнения в эффективности механизмов контроля, которые могут быть предложены на данном этапе с технической и правовой точек зрения. Это отнюдь не означает неэффективности мер раннего предупреждения и выявления угроз, а также международного взаимодействия в области пресечения их распространения. Но в концепции Конвенции прописан *отказ от разработки* информационного оружия, что потребует качественно иных возможностей верификации — увы, отсутствующих на сегодня и в ближайшей обозримой перспективе. Принятие Конвенции, не обеспеченной надлежащими механизмами верификации ее норм, чревато лишь девальвацией ценности идеи, заложенной в основу документа.

Суммируя сказанное, следует признать, что концепция Конвенции и Правила поведения, изначально преследуя весьма масштабные цели, на сегодняшнем этапе сталкиваются с рядом трудностей и вызовов концептуального характера. Во-первых, терминология концепции Конвенции имеет ряд уязвимых мест и нуждается в значительной доработке, в частности в выработке более строгих и однозначных определений ключевых понятий, а также *закрытии брешей*, таких как не затронутая в документе проблема кибершпионажа. Что еще более важно, российские инициативы страдают избыточным упором на роль государства, что ведет к *выпадению* из текста документов других участников информационного обмена — частного сектора, глобальных СМИ, интернет-пользователей, а также посредников, выполняющих волю государств в информационном пространстве. Идеи и принципы контроля государств над сегментами информационного пространства и их ответственности за содержание информационных потоков не подкрепляются решениями правовых и технологических проблем, которые при этом возникают. России необходимо обозначить свой подход к проблемам анонимности в интернете, а также вопросу ответственности за информационные потоки в трансграничной Сети — без этого имплементация принципов концепции Конвенции едва ли возможна. Прописанные в концепции Конвенции задачи по недопущению использования ИКТ в военно-политических целях в ряде случаев опережают нынешние реалии с технологической, международно-правовой и международно-политической точек зрения. Для более успешного продвижения российской идеи на мировой арене целесообраз-

но сужение спектра ее задач в той части, где принципы международного поведения, прописанные в концепции Конвенции, не обеспечиваются работоспособными механизмами контроля верификации. Имеются в виду контроль над содержанием трансграничных информационных потоков, отказ от создания информационного оружия, а также принцип ответственности государств за содержание информации, размещаемой в их информационном пространстве.

ТРАНСГРАНИЧНАЯ КИБЕРПРЕСТУПНОСТЬ И ПОЗИЦИЯ РОССИИ ПО БУДАПЕШТСКОЙ КОНВЕНЦИИ: ПРОБЛЕМА 32B

В европейских странах, США и Канаде одним из факторов, спровоцировавших критику в адрес российских инициатив по обеспечению МИБ, стало наличие в концепции Конвенции положений о международном сотрудничестве в сфере борьбы с трансграничной киберпреступностью. Противодействию этому виду противоправной деятельности в информационном пространстве посвящена глава 4 концепции Конвенции, которая включает в себя статью 10 (Основные меры противодействия правонарушениям в информационном пространстве) и статью 11 (Меры по организации уголовного процесса).

Как известно, Россия на данный момент не является участником ключевого международного механизма противодействия киберпреступности — Конвенции Совета Европы «О киберпреступности», открытой для подписания 23 ноября 2001 г. в Будапеште и вступившей в силу в 2004 г. Несмотря на то что документ носит открытый характер, Россия в конечном счете отказалась присоединиться к нему, в отличие от 37 государств, ратифицировавших Конвенцию по состоянию на 20 сентября 2012 г. Изначально присоединение России к Конвенции было санкционировано распоряжением российского президента от 15 ноября 2005 г. «О подписании Конвенции о киберпреступности» на условиях пересмотра положений статьи Конвенции 32, пункта b[33]. Однако 22 марта 2008 г. вступило в силу распоряжение Президента РФ, в соответствии с которым распоряжение от 15 ноября 2005 г. признано утратившим силу. С тех пор российская сторона не высказывала интереса к конвенции Совета Европы, сосредоточившись на продвижении собственных инициатив в области противодействия кибертерроризму. В ноябре 2010 г. начальник Юридического управления Росфинмониторинга П. В. Ливадный заявил, что «РФ продвигает подход, предусматривающий разработку глобальной конвенции по борьбе с преступлениями в информационной сфере»[34]. При этом характерно, что одна из задач перспективного российского подхода должна будет заключаться «в недопущении расследований [...] на чужой территории», без постановки в известность «правоохранительных органов соответствующего государства»[35].

В данном случае имеется в виду положение Будапештской конвенции, которые вызывает у российской стороны принципиальное несогласие и стало основным препятствием к присоединению России к ее механизму. Статья Конвенции 32, пункт b, предполагает санкционированный доступ уполномоченных органов одного государства-участника к компьютерным данным, хранящимся на территории другого государства, без предварительного получения согласия последнего. «Сторона может без согласия другой Стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получить их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему»[36].

Именно неприятие данного пункта и определяет ту *генеральную линию*, которую заняла Москва в отношении конвенции Совета Европы с 2010 г. и продолжает придерживаться в настоящее время. Представители правительства, МИД и силовых структур в своих работах и выступлениях всячески подчеркивают, что Конвенция была бы неплохим документом, если бы не 32b. По мере созревания российских инициатив по обеспечению МИБ было найдено решение — вырабатывать механизм глобальной борьбы с киберпреступностью собственными силами. Частично

этой цели отвечает концепция Конвенции об обеспечении МИБ, которая содержит ряд положений, затрагивающих вопросы борьбы с трансграничной киберпреступностью. Кроме того, до конца 2012 г. ожидается презентация российской стороной новых инициатив — нового отдельного проекта глобального договора, на этот раз сфокусированного прежде всего на вопросах киберпреступности, либо переработанного проекта Конвенции об обеспечении МИБ.

Критика Конвенции СЕ, которая ведется российскими представителями из числа сотрудников МИД и силовых структур, затрагивает прежде всего данный пункт документа. В частности, утверждается, что это положение Конвенции:

- препятствует эффективному межгосударственному сотрудничеству, обходя согласование с одной из сторон вопроса о трансграничном доступе в ее сети;
- подрывает дух доверительного и слаженного взаимодействия между ее участниками;
- служит формальным прикрытием действий, преследующих не столь дружественные и партнерские действия участников Конвенции.

В рамках последнего пункта предметом опасений представителей российской стороны является угроза разведывательной деятельности европейских и американских спецслужб в российских сетях под прикрытием следственных действий. Например, по словам предыдущего начальника Бюро специальных технических мероприятий МВД России Б. Н. Мирошникова, «лукавая 32-я статья преследует другие цели, а отнюдь не цели расследования компьютерных преступлений»[37].

Аналогичные мнения озвучивались и озвучиваются многими представителями ФСБ, МВД, Совета безопасности РФ и других структур.

Помимо угрозы кибершпионажа, неприемлемым пункт 32b, по версии РФ, делает нарушение государственного суверенитета за счет бесконтрольного вторжения третьей стороны в информационные сети национального государства. Как отмечает профессор МГИМО (У) МИД России А. Г. Волеводз, «в любой стране мира возможно найти конкретного провайдера», который имеет в распоряжении «законные технические механизмы доступа к компьютерным данным, хранящимся за границей», или самостоятельно хранит такие данные на физическом сервере[38]. В итоге, по мнению эксперта, применение статьи 32b к подобным провайдерам создает возможность де-факто бесконтрольного доступа к компьютерным данным в сетях иностранного государства.

Наконец, в последние годы усиливается критика Конвенции в целом как устаревшей и не отвечающей современным тенденциям и изменениям в области трансграничной киберпреступности. Прежде всего отмечается неспособность Конвенции охватить те виды и классы компьютерных преступлений, которые получили развитие за прошедшие 10 лет с момента ее подписания. В список таких киберпреступлений можно включить:

- фишинг;
- создание и использование ботнетов;
- усовершенствованные технологии спама;
- преступления, совершаемые в *виртуальных мирах,* — социальных онлайн-сообществах по типу *Second Life*;
- преступления с использованием социальных сетей — мошенничество, неправомерное завладение персональными данными, воровство аккаунтов (неправомерное присвоение виртуальной идентичности) и т. д.;
- кибертерроризм и использование киберпространства для пропаганды насилия, экстремизма, терроризма.

Некоторые эксперты также включают в этот список массированные организованные кибератаки на объекты критической информационной инфраструктуры, не выделяя их как отдельный феномен киберконфликта, выходящий за рамки киберпреступности[39].

Признавая, что вопрос о нарушении механизмом пункта 32b принципа государственного суверенитета и создании угроз национальной безопасности требует отдельного углубленного исследования, следует, тем не менее, отметить справедливость призывов к модернизации Конвенции СЕ. Необходимость внесения поправок и дополнений в документ действительно назрела. Темпы развития ИКТ и глобальной сети интернет делают невозможным эффективное выполнение своих задач инструментом, рассчитанным на противодействие технологическим вызовам рубежа тысячелетий. Вне механизма Конвенции остается вся совокупность правонарушений, совершаемых в трансграничных социальных сетях, а также преступлений с использованием современных технологий рассылки спама, взлом систем ДБО (дистанционное банковское обслуживание), распространение в интернете информации экстремистского и террористического характера.

Пока на направлении обновления Будапештской конвенции не наблюдается практической активности, что может свидетельствовать о том, что Совет Европы и его государства-участники пока не в полной мере осознали такую необходимость. Так или иначе, если в ближайшие два-три года в Конвенцию не будут привнесены необходимые новации, ее практическое значение как международного механизма противодействия киберпреступности начнет девальвироваться. В таком случае потенциальные инициативы России и ее партнеров могут оказаться более востребованными.

Еще одним слабым местом Будапештской конвенции считается ее *региональный характер* и несоответствие статусу подлинно глобального механизма, который эффективно охватывал бы все международное сообщество. Действительно, на сегодняшний день Конвенции не удалось охватить многие из государств, оказывающих наибольшее влияние на мировую киберпреступность, прежде всего Россию и Китай. Вне Конвенции пока остаются и другие страны, которые на сегодняшний день играют чуть меньшую роль в обеспечении МИБ, однако имеют колоссальный потенциал роста национального IT-сектора, а значит, и взрывного роста рынка киберпреступности. В числе таких стран стоит отметить Индию, Индонезию, Нигерию, Мексику, Вьетнам и другие густонаселенные развивающиеся страны с быстро растущим ИКТ-сектором. В то же время на превращении Конвенции СЕ в глобальный механизм особо настаивают США, которые обеспокоены попытками России выработать ему некие альтернативы.

Официальные лица США все чаще пытаются позиционировать Конвенцию СЕ как безальтернативный и универсальный механизм взаимодействия для стран в любых регионах, включая АТР, особо значимый в этом контексте. Роль развивающихся стран в глобальном информационном обмене, включая прежде всего представителей Восточной и Юго-Восточной Азии, быстро растет, и в будущем будет иметь ключевое значение для международного сообщества. С учетом этого выбор странами региона модели международного взаимодействия по вопросам кибербезопасности и киберпреступности весьма важен как для РФ, так и для США. Пока национальные и региональные подходы находятся в стадии формирования, однако именно страны АТР все чаще поднимают вопрос о модернизации либо замене Будапештской конвенции. Так, возможность разработки и принятия новой конвенции ООН с целью дополнения механизма Будапештской конвенции обсуждалась на Семинаре по акторам-*посредникам* в киберпространстве АРФ, который прошел во вьетнамском Хойане 14–15 марта 2012 г.[40]. Участники семинара не пришли к единому мнению, однако отметили необходимость обновления инструментария Будапештской конвенции.

Подобная ситуация предоставляет России *окно возможностей* по продвижению собственных инициатив и проектов в области глобального противодействия киберпреступности. Однако временные рамки этого окна невелики — процесс

изменения Будапештской конвенции запустить проще и быстрее, чем добиться принятия Конвенции ООН на основе концепции Конвенции об обеспечении МИБ. Кроме того, несмотря на критику и потребность в модернизации Конвенции, процесс присоединения новых членов к ее механизму набирает обороты. Только с начала 2012 г. Будапештскую конвенцию ратифицировали пять государств, включая Грузию и Японию[41], при том, что для Токио процесс ратификации растянулся на 10 лет. В марте 2012 г. было объявлено о запуске третьей фазы Глобального проекта по киберпреступности Совета Европы, целью которого является «содействие применению Будапештской конвенции в глобальном масштабе»[42]. Таким образом, Совет Европы и его ключевые члены, включая Великобританию, уже сейчас четко позиционируют Конвенцию как глобальный, а не региональный инструмент борьбы с киберпреступностью. В этой связи прилагаются соответствующие усилия, включая финансирование программы региональных и страновых семинаров с целью адаптации национальных законодательств к механизму Конвенции СЕ.

Кроме того, интерес к Конвенции проявляет один из главных союзников России по ШОС и ОДКБ — Республика Казахстан. Казахстан с 2011 г. изучает возможность присоединения к конвенции, хотя соответствующее политическое решение в подробностях не прорабатывалось. Учитывая, что Казахстан является вторым по значимости после Китая партнером России по ШОС, любая дискуссия относительно Будапештской конвенции будет воспринята Москвой довольно болезненно. Озабоченность российской стороны в данной области проявила себя в ходе переговоров министра иностранных дел России С. В. Лаврова с главой МИД Казахстана Е. Х. Казыхановым, которые прошли 21 ноября 2011 г. в Москве. Несмотря на то что противодействие новым угрозам фигурировало в повестке переговоров лишь вскользь, российская сторона затронула вопрос казахской позиции относительно противодействия киберпреступности. После этого руководство Казахстана приняло во внимание позицию российской стороны, настаивавшей на необходимости детально проработать возможные последствия присоединения Казахстана к Конвенции СЕ с учетом обязательств Республики перед партнерами по ШОС. На данный момент решение по-прежнему не принято, но сложно ожидать, что Казахстан полностью откажется от рассмотрения такого варианта, особенно в случае модернизации и дальнейшего расширения Будапештской конвенции.

Наконец, любопытна позиция Украины, которая ратифицировала Будапештскую конвенцию еще в 2005 г. с рядом оговорок и заявлений. В 2006 г. Верховная Рада также приняла закон о ратификации Дополнительного протокола к конвенции, однако с тех пор так и не адаптировала свое национальное законодательство к ее нормам. В свете активизации диалога между Киевом и Москвой в последние годы российские власти, вероятно, рано или поздно вернутся к обсуждению украинской позиции в отношении Будапештской конвенции. Что ответит Киев, совершенно неясно — по-видимому, четкое представление о дальнейшей работе по имплементации норм документа отсутствует и в самой Украине.

Еще одним неприятным для Москвы *поворотом сюжета* стала новость о том, что заявку о присоединении к Конвенции СЕ в мае 2012 г. подала Белоруссия[43]. На тему целесообразности присоединения к Конвенции белорусские чиновники высказывались еще в 2007 г.[44], однако нынешнее решение Минска оказалось неожиданностью для Москвы. Любопытно, что речь идет не только об одном из ключевых российских союзников в военно-политических вопросах, но и об элементе Союзного государства России и Белоруссии. Если Минск действительно запустит механизм присоединения к Конвенции, это станет серьезным ударом для Москвы, которой будет сложнее убедить партнеров из отдаленных регионов (АТР, Латинская Америка) в привлекательности своих подходов на фоне потери единомышленников в ключевой зоне влияния — СНГ.

Впрочем, серьезность намерений белорусского руководства по присоединению к Конвенции Совета Европы вызывает сомнения. Открытость и трансграничное сотрудничество, заложенные в основу ее механизма, плохо стыкуются с непрозрачностью системы силовых и правоохранительных органов Белоруссии и тра-

дициональным нежеланием Минска брать на себя какие-либо обязательства в части раскрытия информации, предоставления доступа к своим системам и инфраструктуре. Кроме того, неотъемлемой частью философии Конвенции СЕ является продвижение *неограниченной* свободы в интернете, что сложно связать с курсом белорусских властей, практикующих цензуру в глобальной сети и идентификацию интернет-пользователей по паспортам. Скорее, речь идет о конъюнктурном политическом маневре как части стратегии балансирования Минска между РФ и Евросоюзом, двумя центрами влияния и экономических потоков. Однако подобный торг ставит Россию в уязвимое положение, так как распространение ее среди других партнеров Москвы стало бы дополнительным препятствием к продвижению инициатив, альтернативных Будапештской конвенции.

Вместе с тем, в конечном счете, целесообразность присоединения тех или иных стран к Конвенции СЕ прежде всего определяется тем, насколько эффективно их собственные национальные правовые системы позволяют бороться с киберпреступностью. Этот тезис справедлив и в отношении России. Учитывая, что даже в случае трансформации российской инициативы в конвенцию о МИБ ООН уже в 2013 г. на практическую имплементацию ее механизмов уйдут годы, России в краткосрочной перспективе нужно рассчитывать либо на собственные законы, либо на Будапештскую конвенцию. Между тем на данный момент ситуация на российском рынке киберпреступности представляется тревожной и требующей оперативных изменений.

При этом объективные сложности противодействия киберпреступникам отнюдь не исчерпываются слабостью нормативной базы в РФ. Ключевым препятствием к успешному расследованию киберпреступлений является *трансграничность* преступных групп. Стандартной схемой для широкого ряда киберпреступлений является формирование сообщества, члены которого действуют одновременно с территории различных государств. Количественный и качественный рост банковского сектора и, соответственно, интернет-банкинга, распространение электронных платежных систем и терминалов, общий рост доходов населения РФ и бурное развитие частного сектора сделали достоянием прошлого те времена, когда криминальные атаки осуществлялись только *из* России *против* расположенных за рубежом организаций, объектов, систем. РФ превратилась в самостоятельный, крупный и привлекательный рынок, который с каждым годом привлекает все больше киберпреступников, в том числе из-за рубежа.

В результате российская киберпреступность демонстрирует впечатляющий рост, сдержать который правоохранительным органам в полной мере не удается. В 2010 г. объем средств, заработанных преступниками в российском сегменте интернета в 2010 г., оценивался в 2–2,5 млрд евро[45], а темп роста количества кибератак в том же году оценивался в 80%. Совокупный заработок *русских* киберпреступников в 2010 г. оценивается на уровне 2,5 млрд долл., при этом прогнозировался его рост до 3,7 млрд долл. в 2012 г. и 7,4 млрд долл. США в 2013 г.[46]. Иначе говоря, среднегодовой темп роста показателя приблизится к 100%, а через год доходы *русской* киберпреступности превысят совокупный оценочный доход мирового рынка киберпреступлений за 2010 г. (7 млрд долл. США).

Ситуацию с российским законодательством о спаме и распространении при помощи ИКТ детской порнографии хорошо иллюстрирует пример спамера *Leo Kuvayev* (также известен как *Bad Cow)*, в 2005–2010 гг. известного как «король спама». По словам экспертов[47], в течение нескольких лет Л. А. Куваев, выходец из РФ, проживая в основном в США, создал сложнейшую автоматизированную систему распространения спама, торговли порнографией и вредоносными программами через интернет. Система ежедневно в автоматическом режиме создавала для данной цели, а также для кибермошенничества до тысячи сайтов. Партнерские программы из спамерской сети Куваева *до сих пор* генерируют доход в размере около 30 млн долл. в год. После открытия уголовного дела в США в 2005 г. спамер вернулся в Россию, где оказался недосягаем для американского правосудия, включая Федеральное бюро расследований (ФБР), и продолжил вести свою деятельность,

пользуясь тем, что российские законы *не позволяли привлечь его к ответственности*. Потребовалось пять лет, прежде чем Л. А. Куваева арестовали в России, причем не за совершенные киберпреступления, а по *педофильской* статье 134 УК РФ[48]. Более того, 23 августа 2012 г. стало известно о том, что Верховный суд России снизил срок Куваеву вдвое, с 20 до 10 лет, с отбытием наказания в колонии общего режима[49]. Особенно интересно такое решение выглядит на фоне сегодняшней бурной кампании по борьбе с педофилией и детским порно в интернете.

Не менее тревожной видится ситуация противодействия мошенничеству в интернете. В частности, РФ имеет скудный опыт успешного доведения до суда (не говоря об обвинительных приговорах) дел о мошенничестве в области ДБО. Кроме того, осужденные кибермошенники чаще всего получают наказание по статьям, не имеющим прямого отношения к киберпреступности. Ярким примером является случай хакера Евгения Аникина, который 8 февраля 2011 г. был признан судом виновным во взломе в 2008 г. платежной системы *RBS WorldPay* с нанесением ущерба в размере 10 млн долларов. Сообщники Аникина ранее были экстрадированы в США, где их обвинили в *мошенничестве с использованием электронных средств коммуникации*, за что им грозят тюремные сроки до 20 лет[50]. Сам же Аникин был осужден на условный срок в пять лет за *кражу, совершенную в особо крупном размере* по статье 158 УК РФ, пункт б, часть 4. Разница едва ли нуждается в комментариях. При этом количество преступлений в сфере ДБО в России выросло за 2011 г. в три раза; за одну атаку хакеры в среднем похищают от 600 тыс. до 2 млн рублей[51]. Российская правоохранительная система на данный момент позволяет доводить до суда лишь единицы уголовных дел по таким правонарушениям. Однако только в Москве *ежемесячно* происходит 10–20 *успешных* атак подобного рода, а общее число только зарегистрированных МВД преступлений в сфере информационной безопасности в 2009 г. превысило 15 тыс.[52]. Иными словами, обвинительные приговоры выносятся менее чем по 0,1% дел от числа уже зарегистрированных киберпреступлений.

Схожим образом складывается ситуация с борьбой с DOS и DDOS-атаками. В 2011 г. в РФ DDOS-атакам с использованием ботнетов часто подвергались социальные сервисы, сайты СМИ, интерактивные сообщества на базе платформы *Ushahidi.* Особую тревогу вызывает тот факт, что выбор объектов атаки и характер атак (выбор времени, одновременные мощные атаки на большое количество ресурсов) дает почву для предположений о политическом подтексте подобных акций. Накануне, во время и после выборов в Государственную Думу РФ 4 декабря 2011 г. мощным DDOS-атакам подверглись сайты ведущих СМИ, освещавших выборы (*Коммерсантъ*), *Карта нарушений* — интерактивная онлайн-платформа, позволявшая в режиме реального времени собирать информацию о нарушениях в выборном процессе, блоговый сервис *LiveJournal*, считающийся *цитаделью* российской либеральной оппозиции, и другие ресурсы. Весьма пассивная реакция правоохранительных органов на подобные инциденты отчасти объясняется слабостью российского законодательства в отношении DDoS-атак. Как отмечает эксперт ЦТТИ МГУ имени М. В. Ломоносова А. В. Лямин, «большинство статей [УК РФ], посвященных информационной безопасности, для DDoS *нерабочие*»[53], а виновные в них лица привлекаются к ответственности «исключительно по статье 273 УК РФ»[54]. В итоге слабость законодательных механизмов и пассивность госорганов создают для организаторов подобных атак обстановку безнаказанности.

Впрочем, подобная оценка российской нормативной базы в части борьбы с киберпреступлениями разделяется не всеми специалистами. По словам И. К. Сачкова, «в нашей стране используются те же правовые механизмы, что и на Западе»[55]. При этом «девять составов преступлений, которые в большинстве стран признаны как киберпреступления, у нас отражены в трех статьях главы 28 Уголовного кодекса РФ в совокупности с другими составами [преступлений]», что «дает российскому УК больше пространства для маневрирования» по сравнению с Будапештской конвенцией. По мнению эксперта, преимущество законодательства РФ обусловливается тем, что «в российском УК, в отличие от Будапештской конвенции, отсутствует жесткая привязка к конкретным составам преступлений»[56]. Кроме того, при оценке

темпов роста российского рынка киберпреступности следует принимать во внимание бурный рост интернет-сектора в РФ в целом. В определенной степени расширение масштаба рынка киберпреступности представляет собой естественный процесс, который развивается параллельно с многократным ростом объемов российской интернет-экономики за последнее десятилетие.

Однако данные оговорки не снимают остроты проблемы с киберпреступностью в РФ, равно как и не отменяют потребности в совершенствовании механизмов международного сотрудничества по данным вопросам. Вне зависимости от того, как скоро обновленные российские проекты глобальных механизмов борьбы с киберпреступлениями будут представлены международному сообществу, в ближайшие годы до их возможной практической имплементации Конвенция Совета Европы останется ключевым механизмом в этой области. Возможно, возвращение Москвы к рассмотрению вопроса о присоединении к Конвенции следует увязывать с прогрессом в модернизации последней и наращиванию в ее рамках норм, которые принимали бы во внимание сегодняшние криминальные вызовы в киберпространстве.

Вопрос о соотношении пользы и ущерба от Конвенции СЕ для национальной безопасности и экономики РФ сохраняет свою дискуссионность. Для его критичной и объективной оценки необходимо тщательное исследование, которое позволит оценить негативные и позитивные эффекты от присоединения к Конвенции в экономических категориях. Исследование должно ответить на вопрос, покроет ли потенциальное сокращение объемов потерь российской экономики от действий киберпреступников в результате присоединения к Конвенции возможные потери конфиденциальной информации и ущерб национальной безопасности в результате негативных эффектов применения пункта *32b*, в экономическом выражении. Подобная четкая постановка вопроса поможет развеять существующее в экспертном и деловом сообществах недопонимание позиции российского руководства и спецслужб в отношении Будапештской конвенции. В конце концов киберпреступность представляет такую же угрозу национальной безопасности, а отстаивание принципов государственного суверенитета в современном мире не является абсолютной ценностью, особенно когда речь идет об изначально едином и трансграничном киберпространстве. Конвенция СЕ при всех недостатках не воспринимается в качестве акта, ущемляющего суверенитет, 37 ее членами, включая Японию, Канаду, США и другие государства, которые не участвуют в процессах делегирования государственного суверенитета на наднациональный уровень в рамках Евросоюза. Аналогично, для России вопрос может заключаться не столько в отстаивании жестких принципов, сколько в точном и выверенном *cost-benefit анализе* Конвенции, который позволит более объективно оценить соответствие ее механизма нашим национальным интересам. Важен подход, в рамках которого ни тотальный отказ от Конвенции, ни присоединение к ней не будут рассматриваться в качестве самоцели. Конвенция СЕ могла бы выступать подспорьем для РФ ровно до того момента, когда будут выработаны другие международные нормы по борьбе с киберпреступностью. При этом шанс, что их поддержат зарубежные партнеры РФ, существует и определяется не столько политическими аспектами дискуссии о подходах к МИБ, сколько практической ценностью предлагаемых механизмов. Как отметил в интервью *Индексу Безопасности* директор по вопросам международной политики в киберпространстве британского МИД Джейми Сондерс, если речь будет идти о правовом механизме, «который предложит востребованные на сегодня нормы и более эффективные меры сотрудничества по сравнению с Будапештской конвенцией»[57], такой механизм вполне может быть поддержан Лондоном.

ПЕРСПЕКТИВЫ РОССИЙСКИХ ИНИЦИАТИВ И ВОЗМОЖНЫЕ ПРАКТИЧЕСКИЕ ШАГИ ПО ИХ РЕАЛИЗАЦИИ

Во-первых, официальные выступления представителей РФ на международных мероприятиях, данные о закрытых обсуждениях как внутри страны, так и с партнерами за рубежом позволяют говорить о разумной и гибкой позиции российских

госструктур в части продвижения концепции Конвенции на международной арене. В своем выступлении 1 ноября 2011 г. на Лондонской конференции по вопросам киберпространства глава Минкомсвязи России И. О. Щеголев выразил надежду на то, что российская концепция Конвенции «заложит основу для выработки универсальной конвенции под эгидой ООН»[58]. Таким образом, подача российской инициативы оставляет место для рассмотрения ее в качестве рабочей заготовки, гибкого проекта, который скорее служит базой для дальнейшего диалога по намеченным в нем вопросам, нежели предлагает нашим зарубежным партнерам готовые негибкие решения. В схожем ключе была выдержана речь специального представителя президента РФ по ШОС на Восьмой Генеральной конференции АТССБ — по сути, первая официальная презентация идей Правил поведения в области МИБ ШОС государствам АТР, которые РФ справедливо считает *целевой аудиторией* своих инициатив в сфере обеспечения МИБ[59].

Кроме того, российские государственные органы предпринимают практические усилия по доработке текста концепции Конвенции с учетом отзывов экспертов и наиболее веских пунктов критики со стороны зарубежных партнеров. Такая работа в настоящее время ведется по большей части на площадке российского Совета Безопасности. В частности, текст концепции Конвенции, перспективы его доработки и ключевые критические отзывы в адрес документа обсуждались 6–8 июня 2012 г. на Третьей международной встрече высоких представителей, курирующих вопросы безопасности в Санкт-Петербурге. По итогам встречи не было разработано какого-либо нового варианта текста, однако были учтены отдельные критические замечания и было принято решение продолжить работу в этом направлении. Любопытно, что в преддверии мероприятия секретарь Совбеза Н. П. Патрушев отметил, что задача РФ состоит в том, чтобы заложенные в концепции Конвенции правила стали приемлемы «для большинства государств на начальном этапе», а на конечном этапе распространились бы «в целом, в мире»[60]. Из подобных высказываний можно сделать вывод о том, что российское руководство на данный момент не ставит перед собой задачу максимально быстрого принятия конвенции в рамках ООН. Центр тяжести российских усилий перемещается в область формирования *коалиции поддержки* концепции конвенции, достаточно широкой, чтобы вопрос о принятии конвенции ООН звучал максимально легитимно, даже несмотря на возражения отдельных важных игроков на мировой арене. Не отказываясь от изначальной, весьма масштабной задачи, российский подход в части концепции Конвенции об обеспечении МИБ становится более реалистичным и гибким.

Во-вторых, международное право, на которое зачастую ссылаются западные партнеры Российской Федерации, предусматривает определенные ограничения на распространение информации, подрывающей общественную безопасность. Именно такие действия, по мнению политического руководства и экспертов из России и ряда других стран мира, имели место в 2011–2012 гг. в ходе событий *Арабской весны.* Так, согласно пункту 3 Статьи 19 Международного пакта о гражданских и политических правах, принятого резолюцией Генеральной Ассамблеи ООН от 16 декабря 1966 г., пользование свободой «искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору *налагает особые обязанности и особую ответственность*» и может быть «*сопряжено с некоторыми ограничениями*, которые, однако, должны быть установлены законом и являться необходимыми для:

a) уважения прав и репутации других лиц;

b) охраны государственной безопасности, общественного порядка, здоровья или нравственности населения»[61].

Безусловно, ссылка на норму одного из ключевых актов международного права в области прав и свобод человека придает убедительности позиции российского МИД и самой концепции Конвенции. Проблема, однако, заключается в том, что указанная статья представляет собой норму, которая пока по большому счету не при-

жилась в международной правоприменительной практике, в отличие, скажем, от статьи 51 Устава ООН. С момента принятия Пакта в 1966 г., случаи, когда государства обосновывали бы свои действия в сфере контроля над распространением информации ссылкой на данную норму, крайне редки. Характерно, что эта норма осталась также вне поля зрения правительств Хосни Мубарака, Бен Али, Каддафи, Башара Асада и А. Г. Лукашенко, которые в ходе событий *Арабской весны* активно искали способы ограничить активность оппозиционных движений в социальных сетях на относительно легитимных и понятных мировому сообществу основаниях. Тем не менее апелляция к этой статье вполне правомерна и может использоваться в качестве аргумента в диалоге с зарубежными партнерами РФ. Проблема скорее состоит в том, что положения Пакта, как и любых базовых документов международного права, имеют весьма общую формулировку и оставляют большое пространство для дискуссий. Например, британские власти могли бы считать апелляцию к Статье 19 оправданной для противодействия координации в социальных сетях беспорядков в Лондоне в 2011 г., но отрицать ее применимость к вопросам военно-политического использования ИКТ. Единожды зафиксированные правовые принципы сами по себе далеко не всегда способны переломить политическую волю международных коалиций или отдельных крупных игроков. В этом можно было еще раз убедиться на примере операции НАТО в Ливии в 2011 г., соответствие которой мандату Совета Безопасности ООН широко ставилось под сомнение в мире. Безусловно, данный момент следует учитывать российскому руководству в плане продвижения российских инициатив по обеспечению МИБ.

В-третьих, ошибочно полагать, что Россия одинока в своих подходах, а идея глобального международно-правового документа, охватывающего сразу все измерение информационной безопасности, маргинальна и больше никем не рассматривается. В 2010 и 2011 гг. были опубликованы два издания проекта *The UN Global Treaty on Cybersecurity and Cybercrime* за авторством крупнейшего норвежского киберюриста Штайна Шольберга и его швейцарской коллеги Соланж Гернутти-Эли. Профессор Шольберг в 2007–2008 гг. занимал пост председателя Группы экспертов высокого уровня по кибербезопасности (High Level Expert Group on Cybersecurity), которая была учреждена в 2007 г. для изучения возможностей координации усилий международного сообщества по обеспечению кибербезопасности[62]. Деятельность Группы экспертов должна была дополнять Глобальную программу кибербезопасности Международного союза электросвязи (МСЭ), которая начала действовать в том же 2007 г.[63]

Центральной идеей в проекте Договора является утверждение всеобъемлющего комплексного подхода к регулированию кибербезопасности в международном праве. В этом смысле данная инициатива полностью созвучна российским инициативам. Различие заключается в том, что европейские эксперты по понятным причинам не включают в список угроз распространение информации, которая угрожает подрывом социально-политической стабильности. Куда более явный акцент в проекте сделан на блоке, посвященном киберпреступности. Амбиция авторов состоит в том, чтобы предложить альтернативу определениям Будапештской конвенции и самой Конвенции как таковой. Вместе с тем, согласно комментарию одного из ведущих российских экспертов по киберправу, договор может представлять интерес в контексте отвлеченного теоретизирования и построения идеальных моделей, однако «не представляется перспективным с международно-правовой точки зрения». Подтверждением этой оценки служит тот факт, что с момента выхода проекта Договора в конце 2010 г. не последовало никакой практической реакции на него ни по каналам ООН, ни в рамках каких-либо других рабочих форматов. О самом существовании проекта до конца 2011 г. не было известно российскому МИД, весьма озабоченному поиском единомышленников для российских инициатив.

Кроме того, проекты глобальных норм и договоров в информационном пространстве сегодня прорабатывают многие структуры, в том числе ключевые и крупнейшие международные организации. Как отмечается в выводах программного доклада МСЭ от 2011 г. *В поисках кибермира,* для достижения *кибермира* госу-

дарствам и международным организациям необходимо стремиться к «разработке кодекса поведения в киберпространстве и правовой основы, поддерживающих и продвигающих геокиберстабильность»[64]. Упор в докладе делается прежде всего на декларативные документы и нормы мягкого права, подобные этическим кодексам. В качестве примера таких механизмов приводится Декларация Эриче о принципах киберстабильности и кибермира, принятая в 2009 г. Всемирной федерацией ученых[65]. Однако риторика и тезисы доклада оставляют место и для более традиционных международно-правовых механизмов, в том числе юридически обязывающих договоров и конвенций ООН.

Любопытно, что и сами США — частично под давлением активной российской позиции в области обеспечения МИБ — начинают понемногу играть на поле строительства глобального режима безопасности в сфере ИКТ. На конференции по вопросам киберпространства в Будапеште 4 октября 2012 г. госсекретарь США Хиллари Клинтон выступила с речью, в которой впервые анонсировала заинтересованность и практическую вовлеченность Белого дома в создание среды, где поведением государств в киберпространстве «движут нормы ответственного поведения» и «верховенство права»[66]. Конечно, следует сделать скидку на три принципиально важных момента, которые делают выступление госсекретаря весьма далеким от капитуляции перед российским подходом. Во-первых, речь идет о механизмах *мягкого права*, не имеющих обязательной юридической силы, либо фиксирующих общие обязательные принципы, но не конкретные нормы и механизмы взаимодействия. В этой части госпожа Клинтон скорее приближает постановку вопроса к инициативе Правил поведения в области обеспечения МИБ, но не к концепции Конвенции. Во-вторых, речь по-прежнему идет о киберпространстве, а не об информационном пространстве, а значит, о значительно более узком круге вопросов. Наконец, в выступлении госсекретаря вовсе не прозвучала ООН — единственная рабочая площадка для выработки *глобальных* норм и правил поведения. Вместе с тем были отмечены усилия Вашингтона по налаживанию двусторонних диалогов по вопросам кибербезопасности с Индией, Бразилией и ЮАР. Характерно, что данный перечень включает в себя именно те страны БРИКС, которые Россия активнее всего пытается *перетянуть на свою сторону* в плане подхода к обеспечению МИБ. С учетом этих нюансов следует скорее говорить о продолжении *битвы идей* между сторонниками двух подходов, хотя одна из сторон и пытается модифицировать риторику, частично воспроизводя самые сильные идеи оппонента, но оставаясь в рамках собственной концепции.

В-четвертых, невозможно пытаться отрицать наличие той проблемы, которую призвана решить концепция Конвенции об обеспечении МИБ. Даже если оставить в стороне требующий отдельного исследования вопрос об угрозе информационной войны как манипулировании информацией для подрыва социально-политического уклада в тех или иных государствах, обостряются проблемы киберугроз глобального масштаба, включая кибервойны и саботаж критической инфраструктуры программными средствами. Данная проблематика полностью подпадает под задачи и механизмы в рамках российских инициатив, хотя и составляет лишь их часть. Российский подход к МИБ, что следует особо подчеркнуть, не отметает вопросы кибербезопасности, а просто включает их в более широкую проблематику и не выделяет в качестве самостоятельной сферы регулирования.

Реальность угрозы кибервойн и киберконфликтов в полной мере осознают европейские государства, включая Германию. С 30 ноября по 1 декабря 2011 г. в ФРГ прошла операция *Luekex 2011*, которая представляла собой не что иное, как учебную кибервойну[67]. В рамках операции, в которой приняли участие не менее трех тысяч чиновников имитировались массированные атаки на сайты и информационные системы ряда федеральных и региональных госучреждений. Симуляция кибервойны осуществлялась под наблюдением Национального центра кибероборонны и спецслужб, а подготовка к ней заняла почти два года[68]. Эффективная кибероборона также была включена в число важнейших условий безопасности НАТО в новой Стратегической концепции Альянса от 2010 г.[69]. С 2007 г. после серии атак

на киберинфраструктуру эстонских госучреждений и частных компаний в Таллинне был создан Центр кибероборонь НАТО (CCD COE). В целом, активность государств в сфере военно-стратегического применения ИКТ характеризуется лавинообразным ростом. Если в 1998 г., на момент принятия первой резолюции Генассамблеи ООН по МИБ Генассамблеей ООН серьезными разработками в этой сфере занимались разве что РФ, США и Китай, то сегодня, как уже упоминалось, их ведут более сотни государств, не считая негосударственных субъектов.

Лучше всего о реальной остроте угроз глобальной кибербезопасности свидетельствует их признание той стороной, которая всячески настаивает на несостоятельности российских инициатив, — Вашингтоном. Именно США, согласно американским же экспертам, научным центрам и отчетам госструктур, больше всех страдают от *враждебных актов* в киберпространстве, за которыми якобы стоят государства. Только за последние два года доклады всевозможных американских аналитических центров и институтов приписывают китайским, российским и иранским хакерам систематические атаки на сети Пентагона, попытки кражи данных из сетей ряда федеральных министерств и ведомств, крупнейших оборонных, нефтяных, финансовых и энергетических компаний. В частности, в докладах Пентагона утверждается, что сети ведомства ежедневно выдерживают более шести миллионов попыток неправомерного доступа, в большинстве из которых стоит подозревать российских и китайских хакеров[70].

14 июля 2011 г. замминистра обороны США Уильям Линн III предал гласности данные о крупнейшей успешной атаке «иностранных агрессоров» на сети Пентагона, имевшей место в марте того же года. По словам замминистра, в результате атаки были похищены 24 неизвестными злоумышленниками 24 тыс. секретных и конфиденциальных файлов. Несмотря на отказ прямо назвать автора атаки, источники в Пентагоне весьма прозрачно намекнули на КНР[71]. В ноябре 2011 г. американцы заявили, что взломы геодезических спутников США, якобы имевшие место в 2007 и 2008 гг., «полностью укладываются в логику последних положений военной стратегии Китая»[72]. Тревожной выглядит ситуация с *политически мотивированными* кибератаками на сети частных компаний, обслуживающих объекты критической инфраструктуры. По данным компании *Symantec*, в США только за 2010 г. жертвами таких атак объявили себя 53% операторов объектов национальной критической инфраструктуры[73], практически в каждом втором случае авторство атак приписывается китайцам.

Однако, как можно убедиться на примере операции *Олимпийские игры*, Белый дом далеко не всегда оказывается в оборонительной позиции. По последним данным, разработка серии сложнейших вирусов и внедрение их в сети Ирана и других государств Ближнего Востока стали частью масштабной операции военных и спецслужб США, цель которой в максимальном замедлении иранской ядерной программы. Операция, получившая название *Олимпийские игры*, была спланирована и запущена еще администрацией Джорджа Буша-младшего в 2006 г., резко интенсифицирована после прихода к власти Барака Обамы в 2008 г. и частично продолжает действовать до сих пор[74]. Несмотря на отказ официально признать причастность Белого дома к этой программе и созданию *Stuxnet*, утекающую информацию почти не пытаются опровергать американские власти, так как ситуация выглядит достаточно однозначно.

Развитие военно-стратегического потенциала ИКТ ведется в США и по многим другим направлениям и задачам, зачастую не признаваемым публично. По утверждению Ричарда Кларка, бывшего Национального координатора по безопасности, защите инфраструктуры и контртерроризму США, еще в 2007 г. Израиль провел секретную операцию по уничтожению неопознанного атомного объекта в Сирии, использовав изощренную компьютерную программу для *ослепления* командных систем сирийских ПВО[75]. В результате сирийские силы ПВО были полностью *ослеплены* и не сумели помешать эскадрилье израильских бомбардировщиков, которые успешно разбомбили секретный объект в течение нескольких ночных часов. Данная операция получила в западных экспертных кругах неофициальное название *Фрук-*

товый сад. Г-н Кларк, равно как и другие западные эксперты, не распространяется о том, как Израиль смог разработать подобную программу. Однако, по словам российских технических экспертов в области кибербезопасности, создать такие инструменты без помощи США Израиль на тот момент был не в состоянии, а для операции были использованы наработки американского проекта *Сьютер* (*Suter*).

Оформление кибербезопасности как части *военно-политической* повестки дня происходит в США и на организационно-структурном уровне. Еще в 2009 г. в составе Вооруженных сил США было создано единое Киберкомандование США (USCYBERCOM), в чьи функции входит отражение угроз национальной кибербезопасности, включая *военные киберугрозы*. В результате наряду с тайными операциями превентивные *силовые* действия в киберпространстве получают все более активное развитие в официальных (или полуофициальных) задачах американских госструктур. Перед началом операции *Odyssey Dawn* по обеспечению бесполетной зоны в Ливии в марте 2011 г. американским военным командованием рассматривался вариант нанесения массированного кибердара по инфраструктуре режима Муаммара Каддафи[76]. Подобная опция, несмотря на несоответствие резолюции Совбеза ООН, санкционировавшей бесполетную зону, хорошо укладывается в видение киберпространства как *поля битвы,* которое оформилось в США с принятием Стратегии по действиям в киберпространстве. В ноябре 2011 г. Пентагон подтвердил закрепленное в стратегии право использовать «все необходимые средства», включая военные, «для защиты своей страны, наших союзников, партнеров и интересов»[77]. Таким образом, киберугрозы оказались приравнены к *традиционным* военным угрозам, а в мировой практике появился прецедент права реагировать на киберугрозы использованием обычных вооружений. В августе 2012 г. стало известно о том, что американское Агентство передовых военных разработок (DARPA), стоявшее у истоков создания интернета, объявило тендер на работы в рамках программы *Plan X*[78]. Программа предусматривает создание онлайн-карты киберинфраструктуры США и их потенциальных противников с указанием степеней защищенности и подробных схем стратегических и иных объектов, включая центры оперативного управления, военные базы и склады, объекты транспортной инфраструктуры и системы электроснабжения. Параллельно был объявлен тендер американских ВВС на разработку серии вредоносных программ для «вывода из строя, заражения и взлома операционных систем, серверов и иных сетевых устройств противника», а также «установления временного контроля над киберпространством».

Наконец, США проецируют военно-стратегическое измерение работы с ИКТ и на частный сектор. В августе 2012 г. министру обороны США Леону Панетте была направлена инициатива по расширению полномочий специалистов Пентагона за счет права в отдельных случаях бороться с киберугрозами в сетях других ведомств, а также в частных сетях[79]. А за две недели до этого, в конце июля 2012 г., глава Киберкомандования и директор Агентства национальной безопасности США Кит Александер в своей речи на хакерской конференции *Def Con* в Лас-Вегасе призвал лучших представителей хакерского сообщества идти на службу в возглавляемые им структуры[80].

Упомянутые факты свидетельствуют о том, что Белый дом до сих пор разделяет видение ИКТ, присущее администрации Джорджа Буша-младшего. Суть его сводится к тому, что кибертехнологии — это прежде всего стратегический *актив*, а не *уязвимость* в системе национальной безопасности США. Однако обладая наиболее развитой инфраструктурой ИКТ в мире, Соединенные Штаты оказываются уязвимы для кибератак в беспрецедентной для других стран степени. Дилемма выбора стратегии реагирования на подобную уязвимость долгое время полуспонтанно решалась в пользу укрепления *превентивно-наступательного* потенциала в киберпространстве. Причин было несколько — краткий момент униполярности мира во главе с Америкой в 1990-х гг., казавшийся огромным технологический отрыв США от других стран в сфере ИКТ, отсутствие по-настоящему серьезных киберугроз для самих США, наконец, крайне успешный опыт применения ИКТ для решения военных задач, таких как операция *Буря в пустыне* в 1991 г. в Ираке.

На сегодняшний день мир изменился, однако приоритеты американского подхода к военно-политическому использованию ИКТ остаются прежними, что создает весьма значимую угрозу безопасности глобального киберпространства.

Наращивание США ударного киберпотенциала вкупе с нежеланием обсуждать юридически обязывающие международно-правовые акты в рамках борьбы с киберугрозами тормозит выход мирового сообщества из латентного состояния *войны всех против всех* по Томасу Гоббсу, перенесенной в киберпространство. Государства мира предпочитают готовиться к кибервойнам, а не пытаться исключить их возможность. Эксперты и военные аналитики в Соединенных Штатах уже прогнозируют начало китайско-американской кибервойны на 2015–2017 гг. в связи с вероятным кризисом по поводу статуса Тайваня или спорных островов в Южно-Китайском море[81]. Однако возможные последствия подобного конфликта между государствами с развитыми национальными ИКТ-секторами доподлинно не известны. Поражение критической инфраструктуры в ходе кибервойны способно вызвать непредсказуемые последствия, особенно если речь идет об информационных сетях АЭС, ГЭС, крупных промышленных предприятий, нефте- и газопроводов, логистических узлов, объектов энергогенерации и энергораспределительных сетей. С учетом взаимосвязи элементов глобальной информационной системы, кибервойна в любом случае не может ограничиваться национальными границами изначального объекта агрессии — затронута в той или иной мере будет вся Сеть. Уже по этой причине предотвращение кибервойны является задачей каждого государства, включая как Россию, так и ее партнеров.

Упомянутые факты заставляют задаться закономерным вопросом: насколько уместно игнорировать инициативы по ограничению применения ИКТ в военно-политической плоскости? Как отмечалось выше, США и их западные союзники пока не готовы обсуждать вопросы, связанные с использованием содержания информационных потоков в качестве оружия или военно-стратегического инструмента. Даже если ограничиваться гораздо более узким кругом вопросов кибербезопасности, значительного прогресса не наблюдается и здесь, хотя времени остается все меньше.

Однако, несмотря на данные соображения, на сегодняшний день очевидно, что российская инициатива в той конкретной формулировке и подаче, которые имели место год назад, пока еще не приемлема для *критической массы* наших зарубежных партнеров. Если оставить в стороне рассмотренный ранее вопрос о причинах такой ситуации, на первый план выходит другой вопрос: что делать сейчас?

Менять магистральное направление российского курса в области МИБ, во-первых, вряд ли возможно, во-вторых, контрпродуктивно. Вместе с тем нужно учитывать тот факт, что без определенного сближения позиций и согласования подходов с зарубежными партнерами продвижение российских инициатив вряд ли будет осуществляться должными темпами. Вопрос заключается в том, как предложить ключевым партнерам РФ по диалогу в сфере МИБ приемлемые для них формулы, не отказываясь от конечной цели — построения всеобъемлющего глобального режима обеспечения МИБ. Представляется, что такая работа должна вестись поэтапно, начиная с разрешения наиболее острых противоречий с тем актором, который предлагает и продвигает глобальную альтернативу российскому подходу, то есть с Белым домом. В силу отмеченных выше особенностей доктринального видения США проблем безопасности в сфере ИКТ на нынешнем этапе трудно рассчитывать, что Вашингтон согласится рассматривать тот или иной проект, предполагающий полный запрет на разработку кибероружия и ведение кибервойн, не говоря уже об информационном противоборстве.

С другой стороны, даже среди американского истеблишмента крепнет понимание необходимости запрещения или хотя бы ограничения применения государствами кибероружия в *отдельных* сферах и против *отдельных* типов объектов. Речь, в частности, идет об объектах, имеющих критическое значение для международной безопасности и глобальной стабильности. Прежде всего имеется

в виду инфраструктура, обеспечивающая работу мировой финансовой системы, от которой в равной степени зависят США, Китай, Россия и прочие государства, за исключением нескольких государств вроде КНДР. Такая постановка вопроса, в принципе, отвечает национальным интересам России и всех стран, являющихся элементами глобальной финансовой системы. Вопрос о заключении соглашения о запрете применения кибероружия против информационной инфраструктуры мировой финансовой системы вполне может быть включен в повестку дня российско-американского диалога в дополнение к ведущемуся сотрудничеству по укреплению мер доверия в киберпространстве. Подобные нормы до некоторой степени могут являться развитием постулатов международного гуманитарного права XX в., в частности Гаагских, Женевских конвенций и Дополнительных протоколов к последним.

Безусловно, данным сегментом дальнейшие шаги по укреплению международного сотрудничества в противодействии информационным вызовам ограничиваться не должны. Использование изощренных вирусов, включая включая *Stuxnet, Duqu, Flame, Gauss*, против инфраструктуры Ирана, делает актуальной задачу выработки соглашения, которое запрещало бы целенаправленные кибератаки на информационные системы ОМУ, а также киберинфраструктуру мирной атомной отрасли и наиболее *чувствительных* производств и промышленных объектов. Белый дом едва ли охотно пойдет на обсуждение этого сюжета, по понятным и уже упомянутым причинам. Однако подобная инициатива, в том числе будучи озвученной РФ, оставляет своего автора в выигрышном положении. В данном случае отсутствует привычная почва для критики — размытость формулировок, скрытые возможности для цензуры интернета и прочие недостатки, которые озвучиваются в отношении концепции Конвенции об обеспечении МИБ. Кроме того, идея не просто уместна — она отвечает ключевым озабоченностям международного сообщества в отношении дальнейшего усугубления проблем киберсаботажа. *Stuxnet* всего лишь вывел из строя обогащавшие уран центрифуги, однако следующее поколение подобных программ вполне может быть адаптировано для саботажа на АЭС, химических заводах, хранилищах и системах транспортировки ядерных отходов и других объектах, нарушение нормальной работы которых чревато техногенными катастрофами. Перспектива, которую открывает бесконтрольное использование инструментов киберсаботажа уровня *Stuxnet* уже сегодня — инциденты с человеческими жертвами. В условиях отсутствия согласованного на международном уровне дипломатического и военного алгоритма реагирования и нерешенной проблемы атрибуции такие инциденты могут спровоцировать острейшие дипломатические кризисы и эскалацию конфликтов вплоть до начала военных действий.

Понимание опасности подобного развития событий широко присутствует среди экспертов и дипломатов во всем мире. Если Россия сумеет в правильном ключе подать эту инициативу на международной арене, Вашингтон, решившись ей оппонировать, рискует оказаться в явном меньшинстве и получить поддержку разве что от Израиля. Кроме того, отрицание конструктивного потенциала такой инициативы способно спровоцировать критику со стороны значительной части американского экспертного сообщества. Государства Европы ни *де-юре*, ни *де-факто* не воспринимают операции киберсаботажа по типу *Stuxnet* в качестве адекватных и допустимых инструментов обеспечения национальных интересов. Даже стратегия кибербезопасности Великобритании от 2011 г., в которой ощущается влияние американской парадигматики, отводит место ответным ударам по сетям киберагрессоров и активной обороне в киберпространстве, но никак не превентивному разрушению чужой атомной и промышленной инфраструктуры[82]. В похожем, преимущественно *реактивно-оборонительном* ключе кибервойна понимается и на европейском континенте. Представляется, что основным препятствием к успешному продвижению данной инициативы является скорее в целом настороженное отношение среди западных партнеров к российским инициативам в области МИБ, связанное с вышеупомянутыми спорными моментами в концепции Конвенции. Вместе с тем фундаментальных противоречий приоритетам развитых и развивающихся стран, а также международного сообщества в целом в данном

случае не прослеживается. То есть проблема не носит фундаментального характера, и российской дипломатии требуется лишь преодолеть недоверие наших партнеров при наличии всех *козырей* по сущностной стороне вопроса.

Однако успех этих шагов, в свою очередь, также во многом зависит от того, сумеет ли РФ предложить какие-либо решения применительно к проблеме атрибуции киберугроз и кибератак. Расследование применения *Stuxnet* и его модификаций, длившееся в общей сложности более двух лет, говорит о том, что сами государства без помощи ведущих частных компаний и лабораторий неспособны решать задачу атрибуции сложных и глобальных атак. На острие технического прогресса, хотя и по другую сторону от кибершпионов, киберпреступников и исполнителей актов киберсаботажа, находятся именно крупные частные структуры, которые способны отслеживать даже тщательно замаскированные источники атак. В связи с этим прослеживается еще один потенциальный сюжет, к которому может и должна активно подключиться Россия. Как показала практика, сложные вирусы на Ближнем Востоке изучаются, обнаруживаются и блокируются частными компаниями, которые далеко не всегда сотрудничают друг с другом, а также с государствами, кроме тех, кто сам зовет их на помощь. Ситуация стала понемногу меняться с 2011 г., когда был придан официальный статус сотрудничеству МСЭ с Международным многосторонним партнерством против киберугроз (ИМПАКТ). Только с начала 2012 г. сотрудничество МСЭ и ИМПАКТ позволило выявить несколько серьезных киберугроз — вирусы *Flame* и *Gauss*, а также не получивших практического применения родственников *Flame*. Можно утверждать, что с запуском механизма взаимодействия между ИМПАКТ и МСЭ сотрудничество международных организаций с частным сектором в сфере противодействия глобальным киберугрозам перестало быть спонтанным и начало осуществляться на более-менее системной основе.

Однако потенциал этого механизма пока раскрыт не на 100%, в частности для России, на которую до сих пор не распространяются услуги ИМПАКТ по обеспечению кибербезопасности, в отличие от 144 других государств. При этом в число ключевых участников ИМПАКТ наряду с *Symantec Corporation, F-Secure, Trend Micro, Microsoft* входит и российская *Лаборатория Касперского*, которая фактически стала мировым лидером в части обнаружения изощренных ближневосточных вирусов и противодействия им. Российским госструктурам, безусловно, необходимо в полной мере использовать государственно-частный потенциал (ГЧП) в сфере кибербезопасности, тем более если мы можем задействовать уникальный *центр компетенций — Лабораторию Касперского* — в рамках широкого международного формата.

Удачно проявляющий себя механизм ГЧП должен развиваться и далее, укрепляя свои позиции на площадке ООН. В этой связи перспективным решением представляется создание *Центра предотвращения киберугроз ООН*. Развиваясь на площадке ИМПАКТ, подобная структура может взять на себя функции глобальной площадки по выявлению наиболее серьезных киберугроз и борьбе с ними — ее прообразом уже является Глобальный центр реагирования (ГЦР), составляющий основу механизма ИМПАКТ. Помимо нынешних функций (раннее обнаружение и оповещение о киберугрозах, совместные расследования случаев применения кибероружия, консультации и экспертная помощь пострадавшим государствам) *Центр* может стать официальным разработчиком новых стандартов кибербезопасности, а также вносить вопросы борьбы с развитием кибероружия в повестку Генассамблеи ООН. Россия благодаря сильным позициям и традиционно активному участию в обсуждении вопросов информационной безопасности на площадке Объединенных Наций вполне может сыграть одну из ведущих ролей в укреплении подобного механизма, который отвечает нашим национальным интересам.

С учетом непрекращающегося выявления все новых сложных вредоносных программ в сетях ближневосточных стран опыт и компетенции *Лаборатории Касперского* и других российских структур частного сектора могут стать стратегическим активом РФ на Ближнем Востоке, да и за его пределами. Задача российских госу-

дарственных органов — более системно работать с такими активами, в том числе в рамках задачи формирования режима МИБ. В данном случае России не придется преодолевать сопротивление США, ЕС или других государств, так как ИМПАКТ и государственно-частное партнерство в сфере противодействия киберугрозам воспринимаются в качестве конструктивной и взаимовыгодной инициативы практически всеми странами и международными организациями.

Упомянутыми мерами *точки пересечения* интересов РФ и ее зарубежных партнеров, включая США, по вопросам обеспечения МИБ или безопасности киберпространства не исчерпываются. Их логическим развитием должно стать соглашение о всеобщем запрете на применение кибероружия против критической инфраструктуры невоенных объектов и информационных систем отдельных видов неядерных ударных вооружений. Эти меры являются частью работы по изучению возможностей адаптации и имплементации норм международного гуманитарного права в отношении киберпространства, которую активно ведет РФ. Развитие *Центра предотвращения киберугроз* в дальнейшем открывает возможности для создания *Центра предотвращения информационных угроз ООН,* деятельность которого уже будет распространяться за рамки проблематики *кибер*безопасности. Последняя, к слову, не является более важной, чем вопросы, которые пытается артикулировать Россия. Однако она легче поддается *фиксации* и практической проработке, она более *осязаема* в силу объективных сложностей, которые присущи концептуальным и теоретическим аспектам информационной безопасности в рамках российского подхода и которые рассматривались выше. А следовательно, в том, чтобы пока, *на сегодняшнем этапе* сосредоточиться на формировании международного режима кибербезопасности, нет ничего контрпродуктивного и противоречащего российским интересам. Важно продвигаться там, где это получается на данный момент, и российское руководство на самом деле хорошо это понимает, судя хотя бы по активным переговорам с США по вопросам обмена информацией о киберугрозах и мерах доверия в киберпространстве, которые считаются чисто американским *коньком*. Первым этапом взаимодействия по этой линии стало совместное заявление Климашина–Шмидта в июне 2011 г. и создании российско-американской линии оперативного взаимного информирования о киберинцидентах. Второй этап с подписанием соглашения сорвался в самом начале июня 2012 г., перед встречей двух президентов в Мексике. Однако новая серия обсуждений этих вопросов пройдет уже осенью 2012 г., и рано или поздно приведет к расширению каналов и повестки двустороннего взаимодействия.

Обобщая сказанное, уместно будет привести соображение общетеоретического характера. Суть его заключается в том, что *накрыть* всю проблематику МИБ единым международно-правовым актом в настоящее время едва ли возможно. Необходимо последовательное движение *снизу вверх* — от точечных, узких договоренностей к механизмам более широкого и универсального характера. На фоне стратегической важности задачи строительства режима обеспечения МИБ необходимо помнить о том, что в мировой истории практически неизвестны случаи, когда режимы в сфере разоружения и международной безопасности сразу начинали формироваться с всеобъемлющих глобальных соглашений. При этом также важно, что сфера военно-политического применения ИКТ, не говоря уже о киберпреступности и кибертерроризме, сегодня с трудом поддается эффективному контролю со стороны государств — в отличие от размещения оружия в космосе, вопросов химического и биологического ОМУ.

В данной связи полезен может быть опыт режима контроля над ядерными вооружениями (ЯВ), который в основном сложился за время холодной войны. Его формирование заняло несколько десятилетий, а в части проблематики увязки оборонительных и наступательных стратегических вооружений продолжается до сих пор. Режим контроля над ЯВ вырастал из ограниченных по масштабу и временному горизонту мер, таких как временный договор об ограничении стратегических наступательных вооружений (ОСВ-1) между СССР и США, а также договоров о запрещении испытаний ЯВ в отдельных пространствах. Сверхдержавы

*Пал **Дунай (Венгрия)**, руководитель программы по международной безопасности Женевского центра политики безопасности — по электронной почте из Будапешта:* Я не ожидаю презентации и обсуждения каких-либо «глобальных договоров и предложений по регулированию киберпространства» до конца 2012 г. Конечно, единственное исключение возможно в том случае, если с таким предложением выступят Россия и Китай, подобно тому, как они уже делали в прошлом году перед Конференцией по киберпространству в Лондоне и в ходе нее. На самом деле, мне неизвестно, планирует ли Россия представить какие-либо инициативы помимо тех, которые были изложены год назад в Лондоне и вновь обсуждались на конференции в Будапеште 4–5 октября 2012 г. США и страны Запада, во всей видимости, сейчас не слишком настроены обсуждать подобные идеи. Лондонская конференция, к слову, не считается такой уж успешной, несмотря даже на тот факт, что на ней присутствовали некоторые весьма высокопоставленные персоны, включая шведского министра иностранных дел. То же самое по большому счету можно сказать и в отношении недавней встречи в Будапеште. Возможно, эти конференции все же откроют дверь для более плодотворных обсуждений будущих шагов по укреплению международного сотрудничества в киберпространстве.

прошли через долгие годы изматывающей гонки стратегических ядерных арсеналов и Карибский кризис, прежде чем решились перейти от *выставления потолков* к сокращению запасов ЯВ. Еще недавно применение ЯВ рассматривалось в качестве крайней, но все-таки возможной меры, причем не только оборонительного характера — стоить вспомнить военные доктрины США 1950-х гг. Упомянутая *горячая линия* по киберинцидентам между США и РФ является аналогом канала оповещения об инцидентах с ядерным оружием, который был создан после Карибского кризиса в 1963 г. — за десятилетия до старта масштабного процесса разоружения двух сверхдержав, принятия ряда ключевых договоров в сфере контроля над вооружениями и запрещения ядерных испытаний. Следуя этой аналогии, мы находимся почти в самом начале пути. Сегодня, когда разрушительное оружие может быть создано в течение считанных месяцев и применено в любой точке глобального информационного пространства, десятилетий у нас в запасе нет. Однако законы строительства режимов в сфере международной безопасности действуют и применительно к информационному пространству. Именно поэтому необходимо начинать с соглашений — пусть ограниченных и даже точечных — по наиболее острым и одновременно поддающимся практической проработке вопросам.

ВЫВОДЫ И РЕКОМЕНДАЦИИ

1. До практической имплементации российских инициатив в области борьбы с киберпреступностью в рамках механизмов ООН, очевидно, пройдут годы, в течение которых российский рынок киберпреступности при сохранении *статус-кво* ждет мощный рост. Ситуация во многом обусловливается трансграничным характером киберпреступности, которая все больше ориентируется на Россию как на самостоятельный рынок. Неучастие России в Будапештской конвенции существенно обостряет эту проблему, однако в нынешнем виде Конвенция может нарушать принцип государственного суверенитета и использоваться для скрытого кибершпионажа против РФ. Кроме того, ее нормы устаревают и не покрывают бурно растущие новые сегменты глобальной киберпреступности.

Для критичной и объективной оценки целесообразности присоединения РФ к Конвенции СЕ необходим непредвзятый анализ, который позволит оценить и измерить негативные и позитивные эффекты такого решения в экономических категориях. Необходимо дать ответ на вопрос о том, покроет ли потенциальное сокращение объемов потерь российской экономики от киберпреступности в результате присоединения к Конвенции возможные потери конфиденциальной информации и ущерб национальной безопасности в результате негативных эффектов применения пункта *32b* в экономическом выражении. Подобная постановка вопроса поможет развеять существующее сегодня среди зарубежных партнеров и части российского экспертного сообщества недопонимание позиции российского руководства и спецслужб в отношении Будапештской конвенции. Кроме того, вопрос пересмотра РФ своей позиции в отношении Конвенции может быть увязан с ее обновлением и повышением эффективности ее механизма. Если такие изменения будут иметь место, целесообразен мог бы быть вариант присоединения России к Конвенции на тот срок, пока не будут приняты и имплементированы иные международные механизмы борьбы с киберпреступностью, более отвечающие российским национальным интересам.

2. На сегодняшний день инициативы России и ШОС, изначально преследуя весьма масштабные цели, сталкиваются с рядом концептуальных трудностей и вызовов. Во-первых, их терминология имеет ряд уязвимых мест и нуждается в значительной доработке, в частности выработке более строгих и однозначных определений, а также *закрытии брешей*, таких как проигнорированный вопрос кибершпионажа. Проекты документов страдают избыточным упором на роль государства, который ведет к *выпадению* из их поля зрения других участников информационного обмена, в том числе частного сектора, глобальных медиа, интернет-пользователей и посредников, выполняющих волю государств в информационном пространстве.

В концепции Конвенции и других документах необходимо обозначить подход к проблемам анонимности в интернете, а также вопросу ответственности за информационные потоки в трансграничной Сети, без чего имплементация их принципов едва ли возможна. Прописанные в концепции Конвенции задачи по недопущению использования ИКТ в военно-политических целях в ряде случаев опережают сегодняшние реалии. Для продвижения российских инициатив на мировой арене необходимо сузить спектр задач в той части, где их принципы не подкрепляются дееспособными механизмами контроля и верификации. Такими проблемными вопросами являются контроль над содержанием трансграничных информационных потоков, полный отказ от создания информационного оружия и ответственность государств за содержание информации, размещаемой в «его информационном пространстве».

3. Проблема, которую призвана решить концепция Конвенции об обеспечении МИБ и другие инициативы РФ, стоит весьма остро в глобальном масштабе. Помимо угрозы информационной войны как манипулирования информацией с целью подрыва социально-политического уклада, нарастают глобальные киберугрозы, включая кибервойны и разрушение критической инфраструктуры. Данная

ЛИСТАЯ СТАРЫЕ СТРАНИЦЫ

Современные информационные технологии могут использоваться в качестве оружия. Причем воздействие такого оружия качественно отличается от традиционного, и, соответственно, вопросы его дальнейшего развития, распространения и возможного применения должны стать предметом специальных норм международного права. Вся история развития новых видов оружия начиная от обычного и кончая ракетно-ядерным говорит о том, что международное сообщество в итоге находило разработку таких норм рациональной и необходимой. Проблема, однако, в том, что эти меры разрабатывались чаще всего уже после того, как новое оружие было изобретено и применено.

Международные вызовы информационной безопасности. М.: ПИР-Центр, 2001.

проблематика полностью подпадает под задачи и механизмы в рамках российских инициатив. Российский подход к обеспечению МИБ включает вопросы кибербезопасности в более широкую проблематику, не выделяя их в качестве самостоятельной сферы регулирования.

С учетом взаимосвязи элементов глобальной информационной сети, кибервойна в той или иной мере затронет ее всю. По этой причине предотвращение кибервойн является задачей каждого государства, включая Россию и ее западных партнеров. Однако сегодня международные усилия по формированию режима безопасности киберпространства явно недостаточны. Наращивание США ударного киберпотенциала вкупе с нежеланием обсуждать юридически обязывающие международно-правовые акты в рамках борьбы с киберугрозами тормозит выход мирового сообщества из латентного состояния *войны всех против всех* по Томасу Гоббсу, перенесенной в киберпространство. Государства мира предпочитают готовиться к кибервойнам, а не пытаться исключить их возможность.

4. Вместе с тем в мире крепнет понимание необходимости запрета или хотя бы ограничения применения кибероружия в *отдельных* сферах и против *отдельных* типов объектов. Речь идет об объектах, имеющих критическое значение для международной безопасности и глобальной стабильности. России в данный момент имеет смысл сосредоточить усилия на следующих вопросах:

- выработка и заключение многостороннего соглашения (при особой роли взаимодействия с США) о запрете кибератак на информационную инфраструктуру глобальной финансовой системы;
- заключение на площадке ООН договора/конвенции о запрете кибератак на инфраструктуру ОМУ, а также наиболее *чувствительных* производств и промышленных объектов, разрушение которых чревато техногенными катастрофами;
- присоединение к механизму ИМПАКТ и максимальное усиление своих позиций в рамках этого механизма, включая использование потенциала частных российских компаний (в том числе *Лаборатории Касперского*) в решении глобальных проблем кибербезопасности;
- развитие ИМПАКТ до официальной площадки ООН по противодействию угрозам МИБ — *Центра информационных угроз ООН*, структуры ГЧП, которая объединит крупнейших игроков индустрии кибербезопасности, а также масс медиа. Структура сможет стать официальным разработчиком новых стандартов кибербезопасности, а также вносить вопросы борьбы с разработкой и применением кибер- и информационного оружия в повестку дня Генассамблеи ООН, расследовать случаи применения такого оружия и информировать об информационных угрозах мировое сообщество.
- адаптация ключевых норм и принципов международного гуманитарного права, включая Гаагские конвенции, а также Женевские конвенции и Дополнительные протоколы к ним, к условиям конфликтов в кибер- и информационном пространстве. Это направление может включать выработку всеобщего запрета на применение кибероружия против критической инфраструктуры невоенных объектов.

Проблематика кибербезопасности не является фундаментально более важной, чем вопросы обеспечения МИБ, которые пытается артикулировать Россия. Однако на данном этапе вопросы кибербезопасности легче поддаются *фиксации* и практической проработке, они более *осязаемы* в силу объективных сложностей, присущих концептуальным и теоретическим аспектам информационной безопасности в рамках российского подхода. В силу этого *на сегодняшнем этапе* целесообразнее сосредоточиться на формировании международного режима безопасности киберпространства, что также в полной мере отвечает российским национальным интере-

сам. Представляется, что *охватить* всю проблематику МИБ единым международно-правовым актом на данный момент невозможно, и, следовательно, необходимо постепенное движение *снизу вверх* — от точечных, узких договоренностей к механизмам более широкого и универсального характера, которые на некотором этапе перерастут рамки проблематики кибербезопасности и вместят в себя те вопросы, которые Россия пытается выдвинуть в ранг глобальных приоритетов сегодня. Пока первостепенной задачей должно стать достижение конкретных соглашений в более узкой нише кибербезопасности как первый шаг в последовательном движении из состояния полной правовой неурегулированности ИКТ в контексте международной безопасности к всеобъемлющему режиму обеспечения МИБ.

5. Последнее соображение не вытекает из анализа напрямую и представляет собой развитие предыдущих выводов. Для продвижения инициатив в области обеспечения МИБ России, по всей видимости, необходимы определенные шаги на национальном уровне. Ключевым из них представляется разработка национальной стратегии информационной безопасности (или, возможно, кибербезопасности). Одной из задач такой стратегии должно стать обеспечение поддержки российским международным инициативам за счет формирования видения проблематики кибер- и информационной безопасности в рамках приоритетов национального уровня. Для обеспечения преемственности и единства подхода к вопросам информационной безопасности на национальном и международном уровне такой документ должен решать следующие задачи:

- определять пути совершенствования законодательной базы РФ в области противодействию киберпреступности, особенно в части международного сотрудничества;
- закреплять и обосновывать модель реагирования на агрессивные действия государств и их посредников в информационном пространстве с учетом *проблемы атрибуции*;
- выделять в отдельное направление и подробно регулировать вопросы, которые укладываются в проблематику кибербезопасности (защиту критической инфраструктуры, противодействие актам киберсаботажа, защиту национальных сетей от вредоносного кода и так далее);
- синхронизировать деятельность структур, отвечающих за обеспечение национальной безопасности РФ, по противодействию информационной агрессии, а также закреплять видение и принципы взаимодействия таких структур с российскими и глобальными медиа, частными организациями ИТ-сектора и интернет-сообществами.

В целом, новый стратегический документ должен стать тем *пропущенным звеном эволюции* между Доктриной информационной безопасности 2000 г. и конкретными законодательными актами, отсутствие которого мешает свести российскую государственную политику в сфере информационной безопасности в единый логически цельный комплекс ценностей, задач и средств их достижения. Международная составляющая такой политики от этого выиграет в первую очередь.

Примечания

[1] Department of Defense Strategy for Operating in Cyber Space. July 2011. http://www.defense.gov/news/d20110714cyber.pdf (последнее посещение — 4 октября 2012 г.).

[2] Крутских А. К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы*. http://www.intertrends.ru/thirteen/003.htm (последнее посещение — 4 октября 2012 г.).

[3] Там же.

[4] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей (по докладу Перво-

го комитета (A/53/576). Организация объединенных наций. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement (последнее посещение — 4 октября 2012 г.).

[5] Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. Fifty-third session. First Committee. Distr.: General. 30 September 1998. http://disarmament2.un.org/Library.nsf/1c90cfa42bbb0d6985257631004ff541/663e6453bdaa2e22852576500055027 7/$FILE/A-C1-53-3_russia.pdf (последнее посещение — 4 октября 2012 г.).

[6] Text: Common Security Challenges at Threshold of the 21st Century. USIS Washington File. 1998, September 02, http://www.fas.org/news/russia/1998/98090212_tpo.html (последнее посещение — 4 октября 2012 г.). Также см.: *Крутских А.* К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы. Журнал теории международных отношений и мировой политики.* http://www.intertrends.ru/thirteen/003.htm#2 (последнее посещение — 4 октября 2012 г.).

[7] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей [по докладу Первого комитета (A/56/533)]. A/RES/56/19. Генеральная Ассамблея. http://www.ifap.ru/ofdocs/un/5619.pdf (последнее посещение — 4 октября 2012 г.).

[8] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря. A/60/202. Генеральная Ассамблея. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/65/PDF/N0545365.pdf?OpenElement (последнее посещение — 4 октября 2012 г.).

[9] Fact Sheet. Developments In The Field Of Information And Telecommunications In The Context Of International Security. United Nations Office for Disarmament Affairs. http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf (последнее посещение — 4 октября 2012 г.).

[10] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/RES/60/45. Генеральная Ассамблея. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/490/32/PDF/N0549032.pdf?OpenElement (последнее посещение — 4 октября 2012 г.).

[11] *Крутских А.* К политико-правовым основаниям... http://www.intertrends.ru/thirteen/003.htm (последнее посещение — 4 октября 2012 г.).

[12] Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря. A/65/201. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/469/59/PDF/N1046959.pdf?OpenElement (последнее посещение — 4 октября 2012 г.).

[13] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Доклад Генерального секретаря. A/66/152. Генеральная Ассамблея. http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=R (последнее посещение — 4 октября 2012 г.).

[14] Там же.

[15] Черненко Е. Россия зашла на интернет-форум со своими правилами. *Газета «Коммерсантъ»*. 2011, 1 ноября, http://www.kommersant.ru/doc/1807713/print (последнее посещение — 4 октября 2012 г.).

[16] Шестой международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму», 23–26 апреля 2012 г. Институт проблем информационной безопасности (ИПИБ) МГУ имени М. В. Ломоносова. 2012, 25 апреля, http://www.iisi.msu.ru/news/news56/(последнее посещение — 4 октября 2012 г.).

[17] Там же.

[18] An open internet is the only way to support security and prosperity for all. Foreign Secretary speech at the Budapest Conference on Cyberspace. Foreign&Commonwealth Office. 2012,

October 4, http://www.fco.gov.uk/en/news/latest-news/?id=818554782&view=Speech (последнее посещение — 4 октября 2012 г.).

[19] Russia — U.S. Bilateral on Cybersecurity. Critical Terminology Foundations. Issue 1, 2011. EastWest Institute and the Information Security Institute of Moscow State University. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=130080 (последнее посещение — 4 октября 2012 г.).

[20] О ратификации Соглашения между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Закон Республики Казахстан от 01.06.2010 № 286-IV. http://e.gov.kz/wps/wcm/connect/62b81c00433164d5bac4be06acaf12a7/Z100000286_20100601.htm?MOD=AJPERES&CACHEID=62b81c00433164d5bac4be06acaf12a7&useDefaultText=0&useDefaultDesc=0 (последнее посещение — 4 октября 2012 г.).

[21] Подробнее см. статью в этом номере журнала *Индекс Безопасности*: Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности. *Индекс Безопасности*. 2013. Весна. № 1 (104). С. 78–80.

[22] Три брата Flame. Лаборатория Касперского. 2012,17 сентября, http://www.kaspersky.ru/news?id=207733844 (последнее посещение — 4 октября 2012 г.).

[23] «Лаборатория Касперского» и Международный союз электросвязи обнаружили новый вид кибероружия. Kaspersky Lab. 2012, 28 июня, http://www.kaspersky.ru/news?id=207733770 (последнее посещение — 4 октября 2012 г.).

[24] Вирусы-шпионы для кибервойны. Сделано в США, эффект гарантирован. *Радио Голос России.* 2012, 18 сентября, http://rus.ruvr.ru/2012_09_18/Flame-masshtab-jepidemii-besprecedenten/(последнее посещение — 4 октября 2012 г.).

[25] Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве Министерство обороны Российской Федерации (Минобороны России). http://www.ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (последнее посещение — 4 октября 2012 г.).

[26] Подробнее о проблемах глобальной идентификации в Сети см. статью в этом номере журнала Индекс Безопасности: Якушев М. Международно-политические проблемы идентификации в интернете. *Индекс Безопасности*. 2013. Весна. №1 (104) С. 87–102.

[27] World Federation of Exchanges. NYSE Euronext — NewYork. http://www.world-exchanges.org/member-exchanges (последнее посещение — 4 октября 2012 г.).

[28] NYSE Euronext. September 8, 2004: Testimony of Robert G. Britz, President and Co-COO, New York Stock Exchange, Inc. on «Protecting our Financial Infrastructure: Preparation and Vigilance». before the Committee on Financial Services U.S. House of Representatives Washington, DC.

[29] Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives. January 2003 CRITICAL INFRASTRUCTURE PROTECTION. Efforts of the Financial Services Sector to Address Cyber Threats. http://www.gao.gov/new.items/d03173.pdf (последнее посещение — 4 октября 2012 г.).

[30] Symantec 2010 Critical Infrastructure Protection Study. Symantec. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=CIP_survey (последнее посещение — 4 октября 2012 г.).

[31] *Hedley R. A.* Transnational Corporations and Their Regulation: Issues and Strategies. ABSTRACT. http://instructional1.calstatela.edu/tclim/S09_Courses/HEDLEY-tncs.pdf (последнее посещение — 4 октября 2012 г.).

[32] Черненко Е. Россия продвигает границы в интернет. *Газета «Коммерсантъ»*. 2012, 27 апреля, http://www.kommersant.ru/doc/1924818/print (последнее посещение — 4 октября 2012 г.).

[33] Council of Europe. Convention on Cybercrime, Budapest, 23.XI.2001. http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (последнее посещение — 4 октября 2012 г.).

[34] Россия отказалась ратифицировать конвенцию СЕ о киберпреступности. *Газета «Взгляд»*. 2010. 9 ноября. http://www.vz.ru/news/2010/11/9/445958.html (последнее посещение — 4 октября 2012 г.).

[35] Там же.

[36] European Treaty Series — No. 185. Convention on Cybercrime. Budapest, 23.XI.2001. http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (последнее посещение — 4 октября 2012 г.).

[37] Выступление начальника Бюро специальных технических мероприятий МВД России генерал-полковника милиции Бориса Мирошникова на конференции в рамках Проекта Международного сотрудничества по уголовным делам на тему: «Перспективы международного сотрудничества по уголовным делам, 1 марта 2007. Министерство внутренних дел Российской Федерации. http://www.mvd.ru/reform/interview/show_83370 (последнее посещение — 4 октября 2012 г.).

[38] Волеводз А. Конвенция о киберпреступности: новации правового регулирования. *Правовые вопросы связи*. 2007. № 2. С. 17–25. http://www.mgimo.ru/files/113908/113908.pdf (последнее посещение — 4 октября 2012 г.).

[39] Schjolberg S., Ghernaouti-Helie S. A Global Treaty on Cybersecurity and Cybercrime. Second edition, 2011. http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (последнее посещение — 4 октября 2012 г.).

[40] Co-Chairs' Summary Report. ARF Workshop On Proxy Actors In Cyberspace. Hoi An City, Quang, Nam Province, Viet Nam. ASEAN Regional Forum. 14–15 March 2012. http://aseanregionalforum.asean.org/files/library/ARF%20Chairman's%20Statements%20and%20Reports/The%20Nineteenth%20ASEAN%20Regional%20Forum,%202011-2012/10%20-%20Co-Chairs%20Summary%20Report%20-%20ARF%20Workshop%20on%20Proxy%20Actors%20in%20-Cyberspace,%20Quang%20Nam.pdf (последнее посещение — 4 октября 2012 г.).

[41] CYBERCRIME. Council of Europe. 2012, March 2, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (последнее посещение — 4 октября 2012 г.).

[42] UK supports the Global Project on Cybercrime. Council of Europe. 2012, March 2, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (последнее посещение — 4 октября 2012 г.).

[43] Черненко Е. Белоруссия выбрала интернет побезопаснее. *Газета Коммерсантъ*. 2012, 7 июня, http://www.kommersant.ru/doc/1953059 (последнее посещение — 4 октября 2012 г.).

[44] Киберпреступность не имеет границ. *Экономическая газета*. 2007, 29 мая, http://www.neg.by/publication/2007_05_29_8207.html?print=1 (последнее посещение — 4 октября 2012 г.).

[45] ESET: рынок киберпреступности в России. Итоги 2010 года. *ESET.* http://www.esetnod32.ru/.company/news/?id=35865&year=2011# (последнее посещение — 4 октября 2012 г.).

[46] «Русский» рынок компьютерных преступлений в 2010 году: состояние и тенденции. Москва, 2011. Group-IB. http://www.group-ib.ru/wp-content/uploads/2011/03/GIB-Issl-rynka_2010.pdf (последнее посещение — 4 октября 2012 г.).

[47] Сачков И. Правовые аспекты борьбы с киберпреступностью. Доклад в рамках Специальной программе RIW-2011: Неделя российского интернета, 18.10.2011. http://2011.russianinternetweek.ru/program/(последнее посещение — 4 октября 2012 г.).

[48] Половое сношение и иные действия сексуального характера с лицом, не достигшим шестнадцатилетнего возраста.

[49] Раскин А. Насильнику смягчили приговор. *Expert Online*. 2012, 23 августа, http://expert.ru/2012/08/23/nasilniku-smyagchili-prigovor/(последнее посещение — 4 октября 2012 г.).

[50] За кражу $10 млн российскому хакеру дали условный срок. *BFM.Ru.* 2011, 8 февраля, http://www.bfm.ru/articles/2011/02/08/za-krazhu-10-mln-rossijskomu-hakeru-dali-uslovnyj-srok.html (последнее посещение — 4 октября 2012 г.).

[51] Число преступлений в сфере интернет-банкинга за год выросло в три раза. *DIGIT. Проект РИА Новости*. 2011, 28 октября, http://digit.ru/internet/20111028/385602315.html (последнее посещение — 4 октября 2012 г.).

[52] Семинар Академии народного хозяйства при Правительстве РФ «Компьютерные преступления или что делать, если это случилось в твоей компании». 2011, 3 марта, http://www.globalcio.ru/theme-2011-03-first/(последнее посещение — 4 октября 2012 г.).

[53] Интернет-конференция «DDoS-атаки в России как способ нечестной конкурентной борьбы». *ИА Клерк.Ру*. 2010, 16 декабря, http://www.klerk.ru/buh/articles/205822/(последнее посещение — 4 октября 2012 г.).

[54] Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ. Уголовный Кодекс РФ от 13.06.1996 № 63-ФЗ (принят ГД ФС РФ 24.05.1996) (действующая редакция). http://www.consultant.ru/popular/ukrf/10_38.html#p4556 (последнее посещение — 4 октября 2012 г.).

[55] Сачков И. Интервью с автором. 2012, 27 сентября.

[56] Там же.

[57] Подробнее см. интервью в этом номере журнала *Индекс Безопасности*: Сондерс Джейми. Как избежать эскалации конфликтов в киберпространстве? *Индекс Безопасности*. 2013. Весна. № 1 (104). С. 11–16.

[58] Выступление Игоря Щёголева на конференции по вопросам киберпространства (The London Conference on Cyberspace), Лондон, 1 ноября. Минкомсвязь России. http://minsvyaz.ru/ru/speak/index.php?id_4=42975 (последнее посещение — 4 октября 2012 г.).

[59] Kirill Barsky, Special Representative of the President of the Russian Federation on the Shanghai Cooperation Organization. «The International Information Security as a Global Challenge: The Shanghai Cooperation Organization's Vision». Текст имеется в распоряжении ПИР-Центра.

[60] РФ представит Совбезу ООН конвенцию по IT-безопасности. Digit. Проект РИА Новости. 2012, 5 июня, http://www.digit.ru/state/20120605/392334876.html (последнее посещение — 4 октября 2012 г.).

[61] Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 г. Официальный вебсайт ООН. http://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (последнее посещение — 4 октября 2012 г.).

[62] The High-Level Experts Group on Cybersecurity (HLEG). ITU Official Website. http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html (последнее посещение — 4 октября 2012 г.).

[63] *Schjolberg S., Ghernaouti-Helie S.*. A Global Treaty on Cybersecurity and Cybercrime. Second edition, 2011. http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (последнее посещение — 4 октября 2012 г.).

[64] В поисках кибермира. Хамадун И. Туре (Hamadoun I. Touré), Генеральный секретарь Международного союза электросвязи и Постоянная группа по мониторингу информационной безопасности Всемирной федерации ученых. 2011, январь, http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-R.pdf (последнее посещение — 4 октября 2012 г.).

[65] Там же.

[66] Video: Hillary Clinton's Remarks for the Budapest Cyber Conference. Secretary of State Hillary Rodham Clinton; Budapest, Hungary. U. S. Department of State. 2012, October 4, http://still4 hill.com/2012/10/05/video-hillary-clintons-remarks-for-the-budapest-cyber-conference/

[67] В Германии началась учебная кибервойна. *Lenta.ru,* 2011, 30 ноября, http://lenta.ru/news/2011/11/30/lunex/(последнее посещение — 4 октября 2012 г.).

[68] Там же.

[69] Активное Участие, Современная Оборона. Стратегическая Концепция Обороны и Обеспечения Безопасности Членов Организации Североатлантического Договора. 2010, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-rus.pdf (последнее посещение — 4 октября 2012 г.).

[70] The Pentagon's New Cyber Command. ISN ETH Zurich. 2010, December 20, isn.ethz.ch/isn/Current-Affairs/ISN-Insights/Detail?lng=en&id=125768&contextid734=125768&contextid735=125766&tabid=125766 (последнее посещение — 4 октября 2012 г.).

[71] Pentagon admits suffering major cyber attack in March. *BBC News.* 2011, 14 July, http://www.bbc.co.uk/news/world-us-canada-14157975 (последнее посещение — 4 октября 2012 г.).

[72] Chinese Military Suspected in Hacker Attacks on U.S. Satellites. Bloomberg. By Tony Capaccio and Jeff Bliss. 2011, 27 October, http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html (последнее посещение — 4 октября 2012 г.).

[73] Half of Critical Infrastructure Providers Have Experienced Perceived Politically Motivated Cyber Attacks. Press Release: Symantec. 2010, October 6, http://finance.yahoo.com/news/Half-of-Critical-iw-478930509.html?x=0&.v=1 (последнее посещение — 4 октября 2012 г.).

[74] Подробнее см.: Sanger David E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. New Yorker: Crown Publishers, 2012. Также см. раздел *Книжные новинки* в этом номере журнала *Индекс Безопасности*.

[75] Cyberwar. The Next Threat to National Security and What to Do About It. By Richard A. Clarke and Robert K. Knake. Ecco. C. 12–17.

[76] Schmitt E., Shanker T. U.S. Debated Cyberwarfare in Attack Plan on Libya. *The New York Times*. 2011, October 17, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1 (последнее посещение — 4 октября 2012 г.).

[77] U.S. reserves right to meet cyber attack with force. *Reuters*. 2011, November 15, http://www.reuters.com/article/2011/11/16/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116 (последнее посещение — 4 октября 2012 г.).

[78] Kennedy J. Plan X: DARPA's Cyberwar. Security. PC World. 2012, August 30, http://www.pcworld.com/article/261720/plan_x_darpa_s_cyberwar.html (последнее посещение — 4 октября 2012 г.).

[79] Двойные стандарты США в киберпространстве. *Peacekeeper.ru. Военно-политическое обозрение*. 2012, 13 августа, http://www.peacekeeper.ru/ru/?module=news&action=view&id=15691 (последнее посещение — 4 октября 2012 г.).

[80] Черненко Е. Хакеров зовут на госслужбу. *Коммерсантъ*. 2012, 1 августа, http://www.kommersant.ru/doc/1992500 (последнее посещение — 4 октября 2012 г.).

[81] См. например: Clarke R., Knake R. Cyberwar. The Next Threat to National Security and What to Do About It. New York: Ecco, 2010. C. 134–136. Brenner J. America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. New York: The Penguin Press, 2011. C. 217–219.

[82] The UK Cyber Security Strategy. Cabinet Office. http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy (последнее посещение — 4 октября 2012 г.).

Галия Ибрагимова

СТРАТЕГИЯ КНР В ОБЛАСТИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Китайский стратег и мыслитель Сунь Цзы в своем знаменитом трактате *Искусство войны* выразил главную идею китайской стратегии — *воевать без оружия, побеждать без боя*[1]. Несмотря на прошедшие лета и столетия, мудрость не утратила актуальность. Ведущие мировые державы стремятся вести противостояния с противником бескровными методами, а вместо оружия все чаще используют информационные технологии и ресурсы. Но *пальму первенства* в информационной войне уверенно сохраняет Китай. Об этом свидетельствуют данные и отчеты различных международных и межведомственных комиссий, исследующих тенденции развития современных информационно-коммуникационных технологий (ИКТ) и возникающие в связи с этим угрозы глобальной безопасности.

СОВРЕМЕННЫЙ КИТАЙ В КИБЕРПРОСТРАНСТВЕ: ДИНАМИКА РАЗВИТИЯ И ОСНОВЫ СТРАТЕГИИ

В отчетах и докладах органов различных государств Китай, как правило, с большим отрывом занимает первое место в списке стран, осуществляющих хакерские атаки и акты кибершпионажа. По оценке американских экспертов, в китайской армии существуют специальные подразделения, специализирующиеся на кибервойнах и способные при необходимости вывести из строя большинство объектов информационной инфраструктуры США[2]. Что характерно, Китай не склонен преувеличивать собственные достижения в киберпространстве. Китайские эксперты часто указывают на то, что безопасность информационных систем страны находится лишь на ранней стадии развития и весьма уязвима перед мерами и технологиями, прописанными в киберстратегиях ведущих мировых держав. Руководство Китая опасается в случае масштабной кибератаки потерять контроль над узловыми точками информационной инфраструктуры, чем могут воспользоваться для дискредитации страны внешние силы[3]. Эти опасения небеспочвенны. В *Индексе кибермогущества*, составленном *Economist Intelligence Unit* и консалтинговой компанией *Booz Allen Hamilton*, Китай занял лишь 13-е место[4], а в рейтинге стран с наиболее развитым сектором ИКТ — лишь 36-е[5].

Означает ли это, что данные западных спецслужб о кибермощи Поднебесной противоречат представлениям составителей рейтингов и самих китайцев? Вовсе нет. Китай отдает себе отчет в том, что в случае прямого противостояния с США его армия и вооружения пока не в состоянии обеспечить адекватный ответ. Поэтому для достижения и сохранения паритета с Западом власти активно занимаются разработкой киберсредств, которые в случае нападения на Китай способны вывести из строя всю информационную инфраструктуру противника. Главная слабость КНР заключается в неспособности самостоятельно создавать новые технологии. ИКТ,

функционирующие в Китае, — это, как правило, искусно скопированные и доработанные технологии, ставящие страну на путь *догоняющей модернизации*, пока не способной генерировать собственные разработки[6]. Тем не менее в последнее время наблюдается резкое увеличение инвестиций в сферу кибербезопасности, а реализация собственных проектов в области ИКТ стала приоритетным направлением инновационного развития[7].

В государственной стратегической программе инновационного развития КНР закреплены важные положения о развитии киберпространства и обеспечения его безопасности. Информационная безопасность для Китая — это прежде всего безопасность его инноваций, и в этом важная особенность подхода страны к вопросам информационной и кибербезопасности. Китайская модель инновационного развития основывается на четком следовании национальным интересам, непрерывном расширении научной и технической базы страны, активном привлечении инвестиций в разработку НИОКР, постоянном совершенствовании законодательства в сфере защиты интеллектуальной собственности. В программе признается, что в производстве высокотехнологичных продуктов в области ИКТ Китай все еще зависим от западных технологий, которые при помощи встроенных шпионских программ могут нанести вред всей китайской информационной инфраструктуре, инновационным разработкам и создать угрозу национальной безопасности страны. Снижение зависимости от западных ИКТ рассматривается как одно из важных средств обеспечения кибербезопасности КНР.

В Китае отсутствует единая стратегия развития киберпространства и обеспечения безопасности информационных систем, но это вовсе не означает, что отсутствует концептуальное обоснование значимости проблемы. Основным документом, в котором подчеркивается значимая роль ИКТ в жизни китайского общества, является Всеобъемлющая концепция национальной безопасности Китая[8]. В концепции отмечено, что информация в современном мире не только открывает много возможностей, но и создает угрозы политической, экономической, военной безопасности КНР. Большое внимание в документе уделено интернету как наиболее значимому, но наименее управляемому сегменту глобального информационного пространства.

ИНТЕРНЕТ В КНР: ИСТОРИЯ РАЗВИТИЯ И ИСТОКИ СТРАТЕГИИ РЕГУЛИРОВАНИЯ

Интернет в Китае впервые был запущен 20 сентября 1987 г. Тогда в Пекинском институте физики и высоких энергий профессор Цянь Тяньбай в рамках проекта CANET (Chinese Academic Network) отправил первое электронное письмо из Китая. Сайт института (http://www.ihep.ac.cn) — один из самых старых и наиболее известных в Китае и за рубежом — стал стартовой площадкой для многих государственных и коммерческих веб-страниц[9]. Содействие развитию китайского сегмента интернета оказали учебные заведения Германии и Канады. В октябре 1990 г. была зарегистрирована китайская доменная зона .cn, и в том же году официально открылся сервис электронной почты из этой доменной зоны[10]. В 1994 г. был осуществлен первый выход в интернет через 64 бит/с линию *Sprint*, и Китай международным сообществом был официально признан страной, обладающей полным набором функций интернета. Стремительному развитию интернета в Китае способствовал взятый компартией в 1995–1996 гг. курс на развитие китайской науки и техники, который включал и разработки в области интернета.

В настоящее время интернет в Китае пользуется большой популярностью: в конце декабря 2011 г. количество интернет-пользователей в стране составило 513 млн человек. Количество пользователей, использующих широкополосный доступ в интернет, составляет 93,5 млн человек[11]. Зона .cn стала рекордсменом по количеству зарегистрированных в ней доменов. При этом общее количество вебсайтов, зарегистрированных в доменной зоне .cn, в середине 2012 г. составляло более 2,3 млн[12].

Стремительное развитие и растущая популярность интернета в Китае поставили перед руководством компартии в 1990-е гг. двойственную задачу. С одной стороны, власти страны не хотели упускать из-под контроля ситуацию в стране, с другой — перед ней остро стояли задачи экономической модернизации, внедрения передовых технологий, ослабления остроты социальных проблем. Внутри политической элиты страны созрело понимание того, что решение этих проблем во многом зависит от уровня проникновения ИКТ во все сферы общественной жизни. Интерактивные технологии — действенный инструмент, способный максимально облегчить работу социальных и государственных институтов и создать своеобразную, доселе не виданную систему виртуальной демократии в стране с огромным и разнородным населением.

Но интернет весьма чувствителен к внешним влияниям технологий. Его свободное функционирование в Китае означало бы проникновение идей, нацеленных на дискредитацию политического строя государства. События на площади Тяньаньмэнь в 1989 г. сделали руководство страны весьма чувствительным к современным технологиям. Тогда посредством информационных ресурсов, в частности средств массовой информации, Западу удалось сформировать образ КНР как автократии, где права человека жестко ограничиваются. По этим причинам правительство Китая долго не могло определиться с тем, какую позицию занять по отношению к интернету. Но в 1996 г. государство дало добро на развитие глобальной сети в стране, и интерактивные технологии были включены в официальные планы развития китайской науки и техники[13].

Стратегия Китая по внедрению и развитию интернет-технологий отличалась от западного подхода. «Интернет — это орудие работы, а не средство времяпрепровождения», — этот лозунг, широко распространенный в стране, четко отражает отношение властей к новым средствам массовой коммуникации[14]. Овладение китайцами приемами работы в сети, а также получение информации, полезной для нации, по мнению властей, способны создать новые рабочие места, повысить жизненный уровень населения, ускорить развитие отсталых регионов, сформировать новую прогрессивную китайскую нацию, а значит, сделать Китай самодостаточной державой и помочь ей занять лидирующие позиции в мире во всех сферах жизнедеятельности.

Интернет-стратегия Китая на первом этапе основывалась на заимствовании технологических достижений развитых стран и адаптации их к специфике собственного экономического, политического, социального и культурного развития. На втором этапе китайское руководство приступило к созданию высокотехнологичных индустриальных зон и технопарков, где развивались интернет-технологии и воспитывались технические кадры.

В ноябре 2005 г. в Китае принята Государственная стратегия развития информатизации на 2006–2020 гг. В ней были сформулированы основные направления развития интернета. Важной задачей стало продвижение интернета в народном хозяйстве для корректировки экономической структуры, а также трансформация метода экономического роста и продвижение информатизации для строительства гармоничного общества[15]. Однако в числе первых задач, которые призван решить интернет, стоят повышение качества медицины и доступ широких масс китайцев к образованию. Эти два направления избраны не случайно. Дистанционная медицина позволяет диагностировать заболевания граждан, находящихся в отдаленных регионах и лишенных возможности приехать в центр на обследование[16]. Дистанционное образование оказалось серьезным подспорьем в решении задачи обеспечения всего населения средним образованием. Приоритеты в сфере сетевых услуг отдаются также банковской сфере, электронной коммерции. Правительство поощряет использование интернета для проведения научных исследований и развития бизнеса. Важным направлением политики Китая является внедрение *электронного правительства*.

Для обеспечения широкого доступа граждан к *онлайн*-услугам необходимо было внедрить интернет не только в крупных городах, но и в отдаленных населенных

пунктах. Началась кампания по повсеместному подключению поселков и деревень к интернету. В 2009 г. около 95% городов и поселков имели высокоскоростной доступ к глобальной сети, а жители 92,5% китайских деревень — возможность подключиться к интернету через телефонную линию[17].

Под воздействием государства быстро увеличивается число провайдеров интернет-услуг. Коммерческим провайдерам официально было разрешено заниматься предоставлением интернет-услуг в 1995 г. В настоящее время самыми крупными компаниями, предоставляющими услуги интернета, являются *China Telecom*[18], *China Mobile*[19] и *China Unicom*[20]. Основная инфраструктура китайского сегмента интернета состоит из девяти интернет-провайдеров, в ведении которых находятся все физические каналы, связывающие Китай с окружающим миром.

Китайский сегмент интернета разделен на несколько специализированных сетей, в которые входят:

- научно-исследовательская *China Science and Technology Network* (CSTNet, http://www.cnc.ac.cn); данная сеть объединяет НИИ, государственные научно-технические органы и некоторые академические учреждения;
- образовательная сеть *China Education and Research Network* (CERNET, http://www.edu.cn), объединяющая образовательные учреждения Китая, включая средние школы и университеты в крупных городах страны;
- коммерческие сети; наиболее крупные — *China Net* (http://www.bta.net.cn), государственная сеть, которая охватывает более 50% рынка интернет-услуг в стране и предоставляет интернет-сервис государственным организациям[21], а также *Golden Bridge Network* (GBNet, http://www.gb.co.cn).

Подобная *специализация* китайского интернета облегчает работу пользователям в сети и позволяет быстро ориентироваться во Всемирной Паутине в зависимости от целей и интересов, в то же время сегментация интернета позволяет властям контролировать деятельность *юзеров* и отслеживать все противоправные действия.

Массовое распространение интернета в Китае вовсе не означает, что компартия ослабила над ним контроль. Наоборот, борьба за предотвращение негативных для властей последствий от информации, распространяемой в Сети, лишь усилилась. Прилагаются огромные усилия для эффективной сетевой цензуры. В основном же наблюдение за работой пользователей ведется на местах и начинается уже с момента регистрации пользователя. Для того чтобы стать интернет-пользователем, физическое лицо должно пройти проверку в местном полицейском отделении и предоставить провайдеру справку установленного образца. По некоторым неофициальным данным, кадровые работники Министерства общественной безопасности нередко работают на руководящих должностях в крупных провайдерских фирмах.

Осознавая, что проконтролировать все действия китайских пользователей в сети невозможно, власти перераспределили функции контроля над Сетью между операторами связи и органами власти на местах. Главным органом, контролирующим интернет в Китае, является Министерство промышленности и информатизации. Министерство было создано в 2008 г. для развития в стране интернета, беспроводной связи, производства электронных и информационных товаров, индустрии программного обеспечения. При этом данное министерство несет ответственность лишь за обеспечение технического функционирования интернета и информационных технологий.

Регулирование контента и электронной медиаиндустрии возложено на другое ведомство — Государственное управление по делам радиовещания, кинематографии и телевидения. Оно ответственно за блокирование интернет-провайдерами на централизованном уровне доступа к порнографическим ресурсам и сайтам,

предлагающим азартные игры. Специальные фильтры, которые провайдеры интернета обязаны устанавливать за свой счет, блокируют также доступ к зарубежным ресурсам политического содержания, используя ключевые слова «диссидент», «Тайвань», «Тибет» и др. Они автоматически заменяются на точки, а сами сообщения удаляются. В число ресурсов, подвергающихся цензуре, входит большинство западных СМИ, сайты множества американских университетов, поисковая система *Alta Vista*. Нарушение данных правил влечет серьезное наказание: у провайдеров могут отобрать лицензию на предоставление услуг связи, а частным лицам грозит смертная казнь за публикацию материалов, не угодных правительству.

Китайские законы и нормативные акты, регулирующие развитие интернета, отличаются особой жесткостью. В 1994 г. Госсовет КНР издал Правила регулирования, обеспечивающие безопасность компьютерных и информационных систем, которые дали Министерству государственной безопасности права и полномочия на управление Сетью. В соответствии с правилами правительство имеет право нейтрализовать практически любой неугодный ресурс. К примеру, ответственность предусмотрена за публикацию «материалов, вредящих репутации государства», но интернет-пользователь не имеет никаких способов определения, вреден ли материал или нет (в сводах законов данное понятие никак не расшифровывается).

В соответствии с национальным законодательством, в Китае существует двухступенчатый доступ к интернету. На первом уровне пользователи могут выйти в мировую сеть лишь через магистральные узлы [backbone networks][22]. Существует ограниченное количество подобных ключевых узлов, которые находятся в ведении центральных министерств или групп, имеющих мощную политическую поддержку власти. На китайский интернет-трафик была наложена сложная система файрволов [system of firewalls][23], которая ограничивает доступ к *проблемным*, по мнению государства, внешним ресурсам. В стране успешно реализуется проект *Золотой щит* (неофициальное название — *Великий китайский файрвол*, игра слов по ассоциации с Великой китайской стеной), в рамках которого создана сложная система фильтрации содержимого интернета в КНР. В рамках проекта функционирует система серверов на интернет-канале между провайдерами и международными сетями передачи информации, которая фильтрует информацию. Файрволы применяются китайскими провайдерами для защиты от вирусов и хакеров, а также для блокирования доступа к определенным сайтам.

Китайское государство бдительно следит за тем, чтобы его граждане жили в соответствии с нормами, призванными обеспечить успешное построение коммунизма. Эти нормы подразумевают, что к гражданам не должна попадать *лишняя* информация. Если вебсайт содержит такую информацию, он фильтруется, и доступ к нему из Китая закрывают. Это относится не только к *антикоммунистическим* сайтам (а это большинство мировых ресурсов, например, интернет-энциклопедия *Wikipedia*). Китайские власти применяют репрессивные меры против антиправительственных акций внутри сети. Пересылка секретных или же реакционных материалов по IP-сетям считается государственным преступлением. Наказания для тех, кто нарушает правила пользования интернетом, варьируются от денежных штрафов до лишения права пользования интернетом.

В 2001 г. было организовано Китайское общество пользователей интернета, призванное служить развитию интернета, а по сути реализовывать решения правительства в сфере контроля над глобальной сетью. За годы существования общество разработало и приняло немало документов, регулирующих деятельность интернет-пользователей. Среди них Конвенция об отраслевой самодисциплине в сфере интернета КНР, Правила самодисциплины о запрете на распространение в интернете развратной, порнографической и другой недолжной информации, Конвенция о бойкотировании вредоносных программ, Конвенция о самодисциплине в области обслуживания блогосферы, Конвенция о самодисциплине в области борьбы с сетевыми вирусами, Манифест об отраслевой самодисциплине

в области издательского права в интернете и ряд других документов, призванных стимулировать здоровое развитие интернета[24].

В 2005 г. были введены усиленные меры по регламентированию деятельности граждан в интернете. Так, было запрещено анонимное общение, введена обязательная регистрация сайтов, проведена серия облав на владельцев нелегальных интернет-кафе. С 2006 г. в Китае начало свою работу специальное полицейское ведомство для контроля за интернетом. *Интернет-полицейские* призваны следить за содержанием сайтов, *онлайн*-форумов и социальных сетей. На многих, прежде всего крупных китайских сайтах, чтобы завести свой блог или оставить сообщение на форуме, нужно пройти обязательную регистрацию, при которой необходимо указать свои настоящие личные данные, включая имя, адрес и идентификационный номер. Все эти данные через компьютерный банк данных проверяют на подлинность, и только после этого регистрация считается пройденной.

К корпоративным пользователям всемирной сети предъявляются более жесткие правила пользования интернетом. Любая компания, желающая подключится к интернету, в течение нескольких месяцев проходит тщательную проверку. Определенные послабления со стороны цензоров имеют лишь крупные компании, которым в силу их коммерческой деятельности необходим доступ к более широкому контенту. Действия всех корпоративных клиентов фиксируются, нарушители наказываются. На предприятиях ведется журнал, где аргументируется посещение каждого сомнительного сайта. Распространена практика использования публичной электронной почты, когда группе сотрудников компании присваивается один и тот же адрес, а переадресация корреспонденции производится через системного оператора или дежурного администратора локальной сети[25].

Создать собственный интернет-сайт юридическому лицу также непросто. Каждый онлайн-ресурс должен получить лицензию, выданную Министерством промышленности и информатизации. Для этого компании необходимо иметь солидный уставный капитал. С 2008 г., согласно новым правилам, подавать заявки на получение лицензий на радиовещание или потоковую трансляцию (видео) *онлайн* могут только компании, принадлежащие властям или контролируемые государством. В 2009 г. вступил в силу закон о том, что для регистрации доменных имен в зоне .cn необходимо подавать письменное заявление, в котором помимо всех личных данных надо указывать и номер лицензии предприятия на коммерческую деятельность.

ДРАКОН В СЕТИ: КИТАЙСКАЯ КИБЕРУГРОЗА

Методы контроля, существующие в Китае, вовсе не означают, что интернет в стране отстает от западных тенденций развития глобальной сети. Китайская система управления интернетом весьма гибкая и предусматривает различные послабления для определенных категорий пользователей: ученых, работников СМИ, бизнесменов, в том числе иностранных инвесторов. Китайский рынок интернет-услуг — один из самых быстрорастущих, что особо привлекает внимание инвесторов. Примечательно, что, несмотря на действующую цензуру контента и фильтрацию трафика, большинство китайцев используют интернет для поиска новостей, участия в социальных сетях и развлечений, растет популярность *онлайн*-покупок. На китайский рынок вышли многие западные высокотехнологичные компании. Это обусловлено весьма благоприятными условиями, которые создают власти Китая. Поощряются научные и прикладные исследования зарубежных компаний в КНР, внедряется система так называемых *информационных портов* — зон свободного таможенного и налогового регулирования, ориентированных на развитие инновационных технологий, электронной коммерции и информатики.

Активное привлечение западных технологий и иностранных инвестиций вовсе не означает, что они свободно ведут свою деятельность в стране и неподконтрольны власти. Госсовет КНР рассматривает интернет как важный объект государственной инфраструктуры, который должен находиться в рамках суверенного

управления Китая. Посягательства на китайский сегмент интернета со стороны внешних сил рассматриваются как угроза национальной безопасности. Иностранные граждане и компании, находящиеся в КНР, при пользовании глобальной сетью должны следовать нормам законодательства и требованиям властей. Любое иностранное юридическое лицо, перед тем как войти на китайский рынок, принимает правила игры китайского правительства и вынуждено действовать в соответствии с ними[26]. Так, компания, специализирующаяся на предоставлении услуг в сфере ИКТ, прежде, чем выйти на рынок, обязана получить лицензию на свою деятельность в Министерстве промышленности и информатизации, так же как и любая китайская компания. Именно из-за отсутствия такой лицензии у китайского подразделения компании *Google* в самом начале работы возникли проблемы.

Еще одно требование Госсовета КНР к иностранным компаниям — это фильтрация трафика и недопущение распространения информации, способной дискредитировать власть. В данной связи показателен инцидент с *Google*, когда весной 2010 г., невзирая на многочисленные предупреждения госструктур, интернет-поисковик отказался фильтровать в сети запросы китайских пользователей. В ответ Китай обвинил *Google* в нарушении *письменного обещания* о подчинении китайским законам, сделанного компанией при выходе на китайский рынок. В ответ компания заявила, что перенаправит китайских пользователей на нецензурируемые страницы своего гонконгского сайта. В защиту поисковика выступил представители Белого дома США, выразив обеспокоенность невозможностью разрешить конфликт и нарушением свободы слова в Китае. Это обострило и без того непростые отношения США и КНР[27]. Политическая подоплека произошедшего скандала позволила обрести мощные рычаги сдерживания китайской экспансии, в частности экспорта ИКТ на мировые рынки, за счет обвинений в отсутствии демократии и свободы слова в Китае, а корпорация *Google* приобрела отличный административный ресурс в Вашингтоне.

Открытость Китая для привлечения передовых западных ИКТ, тем не менее, носит односторонний характер и проявляется главным образом в восприимчивости к передовому зарубежному опыту в этих областях. Собственные разработки широко не афишируются, а между тем благодаря своей относительной дешевизне они активно завоевывают мировой рынок. Продукция, произведенная в Китае, уже давно не вызывает того пренебрежения и недоверия, которые импортеры и рядовые покупатели испытывали еще несколько лет назад при виде надписи *Made in China*. Ныне огромный ассортимент инновационной продукции, начиная от ноутбуков, мобильных коммуникаторов, *iPhone*, GPS-навигаторов, не уступает европейским, американским и японским аналогам. Например, китайская компания *Huawei Technologies* — одна из крупнейших в стране, специализирующаяся в сфере телекоммуникаций. Компания занимает ведущие позиции в мире по изготовлению ноутбуков, оборудования беспроводных сетей, программного обеспечения. Продукцию компании используют 35 из 50 крупнейших мировых операторов связи. Американские военные аналитики причисляют *Huawei Technologies* к главной угрозе безопасности США не только в информационной, но и в военной сфере. Это обусловлено тем, что компания поддерживает тесные связи с китайскими военными. В частности, основатель и бессменный глава *Huawei Technologies* Жень Чженфей в молодые годы служил в Народно-освободительной армии Китая (НОАК). На основе этого и многих других подобных фактов делаются выводы о том, что в производимых компанией *Huawei* технологиях, поставляемых в том числе в США, встроены аппаратные закладки и другие вредоносные шпионские программы[28].

Распространение вредоносных программ — не единственное зло, которое приписывают Китаю в киберпространстве. В отчетах западных разведслужб КНР называют одной их основных стран, откуда исходят угрозы информационной безопасности. Китаю не удается, как прежде, показывать свое невежество и невиновность при проведении кибератак и разведки в киберпространстве США. По данным компании *Northrop Grumman*[29], которая занималась подготовкой отчета для американо-китайской комиссии по отношениям в области экономики и безопас-

ности[30] *«Занимая информационную высоту: возможности Китая по проведению компьютерных сетевых операций и кибершпионажу»,* в китайской армии уже есть подразделения, специализирующиеся на ведении операций в киберпространстве. Существование подразделения кибервойск, которое носит название *Голубая кибермия*, открыто признал министр обороны Китая Генг Яншенг[31]. По оценке американских экспертов, их общая численность может составлять 30 тыс. военнослужащих. В докладе отмечается, что за последние 10 лет было зафиксировано множество случаев проникновения в информационные системы США, в результате которых Китай овладел коммерческими и военными данными. Обширные возможности КНР в области кибершпионажа объясняются активной разработкой киберсредств, которые финансируются со стороны правительства[32].

Эффективность китайских киберподразделений обусловлена тесным сотрудничеством между правительственными структурами, военными и хакерами. Китайские военные видят успех современных боевых действий в способности контролировать информацию и информационные системы противника. Руководство Народно-освободительной армии Китая (НОАК) рассматривает компьютерные сетевые операции как важный элемент информационного противоборства, и стремится объединить все элементы информационной войны (электронные и неэлектронные, наступательные и оборонительные) в единую систему[33]. В отчете компании *Northrop Grumman* отражены конкретные доктринальные намерения, а также сведения о финансовой поддержке Китаем систематического кибершпионажа. Основные положения стратегии информационной войны отражены в Военно-политическом руководстве Китая. Они были внесены в документ в 2002 г., когда НОАК объявило о возрастающей необходимости противостоять врагам в условиях высокотехнологичных войн. Тогда же были сформулированы основные направления оборонной политики КНР, где особый акцент сделан на модернизацию вооруженных сил за счет их информатизации. В документе впервые появилась формулировка «противостояние в локальных войнах в условиях информатизации вооруженных сил», обусловливающая необходимость преобразования вооруженных сил Китая[34].

В рамках НОАК существует детально разработанная доктрина о нападении на компьютерную инфраструктуру противника. Пекин делает ставку именно на этот вид оружия, поскольку по остальным компонентам настолько уступает США, что не надеется сократить разрыв в ближайшие годы. НОАК вербует в свои подразделения некоторых хакеров, а также может использовать их для проникновения в иностранные компьютерные сети. Вывод из строя сетевой инфраструктуры противника, рассчитывают в НОАК, может *ослепить* и задержать мощнейшую в мире американскую армию, что позволит Китаю выиграть время и предотвратить одномоментный полномасштабный удар[35].

Примером проникновения китайских хакеров в американскую информационную инфраструктуру является беспрецедентное по масштабам отключение электроэнергии на северо-западе США в 2003 г. В результате выхода из строя энергосети пострадали около 50 млн человек в штатах Огайо, Нью-Йорк, Мичиган, а также в некоторых штатах Канады. По данным американских спецслужб, за этим отключением стоял Пекин, испытывавший возможности своих киберподразделений. Еще один громкий скандал разгорелся после взлома китайскими хакерами учетных записей нескольких сотен пользователей почтового сервиса *Gmail* компании *Google*, в том числе аккаунтов высокопоставленных американских чиновников. Взлом начался с сообщения, отправленного сотруднику *Google* через программу *Microsoft Messenger*. Нажав на ссылку, сотрудник зашел на зараженный сайт и невольно предоставил злоумышленникам доступ к своему компьютеру, а затем и к компьютерам разработчиков в штаб-квартире компании. Хакерам удалось получить контроль над хранилищем разработок соответствующего отдела[36].

Для расширения возможностей Китая в киберпространстве НОАК активно взаимодействует с коммерческими организациями и сферой образования, что способствует получению доступа к передовым исследованиям и технологиям, в том числе к телекоммуникационным системам военного и двойного назначения. В 50 китай-

ских университетах национальное правительство финансирует различного рода программы, направленные на поддержание исследований в области организации и проведения кибератак и кибероборонь, в том числе связанных с проведением информационной войны. Зачастую эта работа осуществляется посредством взаимодействия с зарубежными партнерами, проводящими исследования в сфере критических технологий[37].

Впрочем, китайские хакеры зачастую организуют атаки на киберпространство иностранных государств самостоятельно и без ведома чиновников. Первой организованной группой китайских хакеров считается группировка *Зеленый отряд*. Она была основана в 1997 г. и существовала как форум для любителей сетевых технологий, которые обменивались опытом по взлому различных систем сетевой защиты. Хакеры из этой группы сыграли ключевую роль в организации кибервойны против Индонезии в 1997 г. Причиной кибератак стали антикитайские погромы в Индонезии в 1998 г., возникшие после финансово-экономического кризиса. Предпосылкой вспыхнувших волнений стал тот факт, что проживающие в Индонезии выходцы из Китая практически полностью взяли под свой контроль послекризисное распределение продовольствия на большей части территории страны[38]. Суть организованной *Зеленым отрядом* кибервойны заключалась в том, что хакеры группировки вывешивали инструкции о том, как атаковать индонезийские правительственные сайты, засылая на их серверы многочисленные электронные письма. Более продвинутые члены группы взламывали сайты и размещали на них записи, призывающие остановить атаки на *хуацяо* — выходцев из Китая. Пик кибератак пришелся на национальный праздник Индонезии — 17 августа, День независимости. Джакарта тогда обвинила официальный Пекин в организации кибервойны.

Китайские хакеры называют себя *хункэ* (*красный гость*) по аналогии с китайским словом *хакер — хэйкэ* (*черный гость*). В 1999 г., после того как американская авиация по ошибке разбомбила посольство КНР в Белграде, они организовали атаки на американские правительственные сайты, в результате которых был впервые взломан сайт Белого дома. Аналогичные действия были предприняты и в мае 2001 г., когда над островом Хайнань столкнулись китайский истребитель и американский самолет-разведчик. По подсчетам самих китайцев, тогда было взломано 1036 американских сайтов, включая 18 военных и 39 правительственных[39].

Китай весьма критично относится к существующему международному режиму управления интернетом, где основные функции по присвоению имен и адресов интернета закреплены за подотчетной США Корпорации по распределению имен и адресов (ICANN). На различных международных форумах, где обсуждаются вопросы управления интернетом, представители Китая всегда жестко критикуют деятельность ICANN, обвиняя ее в пособничестве американцам. Неприятие Китаем деятельности ICANN особенно усилилось после выдачи корпорацией домена .tw Тайваню, официально рассматриваемому Китаем в качестве провинции в составе национальной территории[40]. Главное требование КНР заключается в роспуске корпорации и создании подлинно международной организации, управляющей интернетом под эгидой ООН. В сентябре 2011 г. Китай, Россия и другие страны представили Генеральной Ассамблее ООН проект Правил поведения в области обеспечения международной информационной безопасности и призвали к тому, чтобы страны в рамках ООН провели обсуждение по этому документу и достигли договоренности в международных правилах и нормах всех стран по действиям в информационном пространстве. Предложенный документ призывает к упорядочиванию международных правил в сфере сетевой безопасности и в корне отличается от инициатив в области информационной безопасности, выдвигаемых США и Евросоюзом, где в случаях, угрожающих национальной безопасности, допускается проникновение госструктур в международные информационные сети.

Шанхайская организация сотрудничества (ШОС) — еще одна площадка, которую Китай стремится использовать для регулирования интернета и обеспечения безопасности информационных систем. В частности, вопросы информационной безопасности нашли отражение в заявлении глав государств — членов ШОС

по международной информационной безопасности от 2006 г. на саммите в Шанхае, Екатеринбургской декларации ШОС от 2009 г.[41] и Ташкентской декларации ШОС от 2010 г. В перечисленных документах информационная безопасность рассматривается как важный фактор обеспечения государственного суверенитета, национальной безопасности, социально-экономической стабильности[42].

Однако в вопросе управления интернетом Китай зачастую не ограничивается лишь декларативными документами и намерениями, а переходит к конкретным предложениям и действиям. В частности, Китай предлагает увеличить контроль государств над архитектурой глобального управления интернетом с помощью создания альтернативной версии системы доменных имен — DNS-расширения для автономного интернета[43]. Основные цели внедрения системы альтернативных доменов — снижение зависимости от глобального интернета и создание *автономного интернета*, функционирующего в рамках одного государства. Это позволит пользователям снизить зависимость от иностранных доменов, таких как .com, .net и других, а правительству Китая обойти ICANN и искоренить официальную систему доменных имен в пользу национальных систем. Чтобы не нанести вред существующей системе доменных имен, прежде чем будет создано множество AIP-сетей, каждая страна может независимо от других создать AIP-сеть и подключиться к интернету по исходной ссылке, считают китайские власти. Предполагается, что при таком подходе возможно будет также объединять сети двух и более государств, создавая единую AIP-сеть. Это позволит улучшить *масштабируемость* интернета. Помимо этого, определенные страны смогут ввести лучший контроль над местными сегментами интернета. Китай неоднократно озвучивал эту инициативу на международных форумах по управлению интернетом, а в июне 2012 г. официально подал заявку в Инженерный совет интернета на введение нового стандарта на «расширение DNS для автономного интернета»[44].

КИТАЙСКАЯ ГОСУДАРСТВЕННАЯ ПРОПАГАНДА И СОЦИАЛЬНЫЕ СЕТЕВЫЕ СЕРВИСЫ

Китайские власти видят в интернете и современных ИКТ не только средство устрашения противников, но и большие возможности для формирования позитивного имиджа страны на международной арене. В стране создано специальное Административное бюро по пропаганде в интернете, созданное при Информационном агентстве Государственного совета КНР. Оно направляет и координирует государственную пропаганду в Сети. Еще несколько лет назад основными проблемами развития интернета в Китае были недостаток сайтов, созданных непосредственно в Китае, и дефицит контента на китайском языке. Большинство существовавших в стране печатных и электронных СМИ не имели собственных сайтов в интернете и не были представлены широкой аудитории. Ситуация начала меняться в начале прошлого десятилетия, когда Госсовет КНР осознал, что интернет — это удобный механизм реализации определенных политических и социальных программ. Началось широкое инвестирование не только в масс-медиа на китайском языке, но и в расширение китайских иноязычных СМИ.

На первом этапе власти стимулировали создание интернет-сайтов наиболее крупных информационных агентств, расширили сетку их вещания и распространения. На втором этапе было увеличено количество зарубежных корпунктов государственного информационного агентства *Синьхуа* до 186 и расширена сфера его деятельности на спутниковое и интернет-телевидение. Не менее важной задачей стал запуск китайских СМИ в интернете на иностранных языках, что позволило жителям различных стран и континентов получать информацию из Китая *из первых рук*. Центральное телевидение Китая *CCTV* запустило вещание на английском, французском, испанском, русском, арабском языках, наняв для этих целей более 100 новых иностранных сотрудников.

В 2009 г. медиахолдинг *Жэньминь Жибао* выпустил англоязычную версию газеты по международной проблематике *Хуаньцю Шибао*, которая стала вторым в Китае

Нандан ***Унникришнан****, директор по евразийским исследованиям, старший научный сотрудник Исследовательского фонда Observer, Рахул* ***Пракаш****, младший научный сотрудник, Институт исследований безопасности, Исследовательского фонда Observer — по электронной почте из Дели:* В киберпространстве эффективная оборона невозможна без создания потенциала нападения. К примеру, для того чтобы пресечь кибератаку, государству может быть необходимо вывести из строя компьютерные сети за пределами его национальной территории. Например, Индии на случай конфликта с Китаем необходимо заранее готовиться к возможной кибератаке, нацеленной на выведение строя сетей системы военного командования и управления. Обеспечение информационного превосходства за счет вывода из строя сетевых систем противника, отвечающих за управление, связь, сбор и передачу данных, наблюдение и разведку местности, является центральным элементом китайской стратегии кибервойны, которая органично вписывается в общую военную стратегию КНР. Другим вероятным противником в киберпространстве для Индии является Пакистан, с территории которого ранее осуществлялись кибератаки, нацеленные в числе прочих на индийские органы безопасности. Можно ожидать, что индийские военные готовятся к отражению подобных угроз китайского или пакистанского происхождения.

ежедневным изданием на английском языке после *China Daily.* Данные издания начали активно представлять себя, в том числе в интернете, что резко увеличило аудиторию их читателей по всему миру. Важным этапом в *завоевании* глобального информационного пространства стала практика приобретения долей в иностранных СМИ. Так, в июле 2009 г. владелец пекинской медиакомпании *Xiking Group* заявил о намерении приобрести британский телеканал *Propeller TV* и создать на его основе двуязычный англо-китайский проект, ориентированный на освещение Китая и пропаганду китайской культуры. Увеличение китайских масс-медиа в интернете, рассчитанных на зарубежную аудиторию, создает возможности для властей Китая усилить пропаганду на зарубежные государства и создать иллюзию многообразия источников информации и плюрализма мнений в Китае[45]. Данные тенденции объективно способствуют усилению позиций КНР в глобальном информационном пространстве.

Вместе с тем китайцы начали активно использовать интернет для противодействия критике, звучащей в адрес Китая извне. После событий в 2008 г. в Тибете и в Синьцзян-Уйгурском автономном районе (СУАР) в 2009 г. в западных СМИ было опубликовано множество негативных и не всегда полностью достоверных материалов о действиях китайских властей. Китайские пользователи стали размещать на популярных в стране интернет-порталах *Sina.com* и *China.com* ссылки на конкретные искажения с требованиями опровержения. Был даже создан специальный сайт *Anti-CNN.com*. В результате активной позиции китайских блогеров удалось добиться извинений от некоторых западных СМИ. Таким образом, в современной китайской внешнеполитической пропаганде проявляется стремление Пекина перехватить инициативу, действовать не в ответ на иностранные выпады, а на упреждение, порой даже в наступательном ключе[46].

Большой популярностью в Китае пользуются ведение блогов и участие в социальных сетях. При этом большая часть блогов пишется именно на китайском языке. *Facebook*, *Twitter*, *Livejournal* и другие иностранные социальные веб-сервисы блокируются в стране, поэтому основным ресурсом, на котором ведутся блоги, явля-

ется *Sina Weibo*, который занимает третье место по популярности в Китае. В китайской сегменте интернета существует свыше миллиона форумов, зарегистрировано 220 млн блогеров. Каждый день посредством социальных сетей, блогов, форумов публикуется свыше трех миллионов записей, более 66% китайских пользователей интернета часто выкладывают в сети свои записи, комментируют, жалуются или выражают свою точку зрения на разные темы. Новые функции и новые услуги, предлагаемые интернетом, предоставили более широкое пространство для выражения людьми своих взглядов[47]. Вторым по популярности социальным ресурсом в КНР является социальный портал *51.com*. На нем зарегистрировано 120 млн пользователей. Ежедневно на сайте регистрируются 100 тыс. новых пользователей. Это привлекает инвесторов во всем мире. *Zhanzuo.com*, на котором зарегистрировано семь миллионов пользователей, — еще одна популярная социальная сеть в Китае. Этот ресурс в 2007 г. планировал купить владелец *Facebook* Марк Цукерберг за 85 млн долл., однако стороны так и не пришли к компромиссу, и сделка сорвалась.

В отношении социальных сетей и блогов власти Китая проводят ту же политику тотального контроля, что и в отношении других интернет-ресурсов. Блогхостингам запрещено предоставлять услуги пользователям, не оставившим при регистрации свои подлинные и полные данные. Регистрация пользователей под псевдонимами запрещена. Причем авторизованы в блогосфере Китая должны быть и комментарии — анонимные мнения также вне закона. Для усиления контроля над социальными сетями интернет-сервис *Sina Weibo* ввел в действие новые правила для предотвращения распространения в сети слухов и призывов к акциям протеста. Все 324 млн человек, зарегистрированных в этой социальной сети, получили на свой счет 80 баллов, которые будут отниматься за нарушения правил. Штрафы планируется налагать «за призывы к нелегальной деятельности, нарушению порядка путем создания незаконных организаций», а также «к организации неразрешенных протестов, демонстраций и собраний». Блогеры понесут наказание и за распространение слухов, «затрагивающих честь Китая и подрывающих стабильность в обществе». При исчерпании лимита в 80 баллов аккаунты пользователей будут удаляться[48].

Несмотря на существующие меры контроля социальных ресурсов, китайские пользователи находят способы, чтобы обойти их. Так, для входа *Facebook* и *Twitter* широко используются прокси-серверы и другие ресурсы, позволяющие обходить цензуру. Для обсуждения социально-политических вопросов используются слова, на первый взгляд не имеющие отношение к политике. Например, опальному политику Бо Силаю присвоили имя *помидор*. Его арестовали и отстранили от должности в марте 2012 г. по подозрению в коррупции. Его главный противник, премьер-министр Вэнь Цзябао, получил в блогах кличку *телепузик*. Вместо имени китайского художника-диссидента Ай Вэйвэя в интернете употребляют схожий по написанию иероглиф *любовь к будущему*, а историю слепого адвоката Чэнь Гуанчэна, сбежавшего из-под домашнего ареста и получившего убежище в США, блогеры обсуждали при помощи иероглифа *Шоушенк* (отсыл к голливудскому фильму «Побег из Шоушенка»). Так, при помощи использования каламбуров, омонимов, аббревиатур китайских названий на английском языке блогеры обсуждают важные политические процессы, стараясь не привлекать внимание цензоров. Поскольку эти методы общеизвестны, то и цензура их учитывает, часть из закодированных сообщений уже удалены из сети[49], но удалить все комментарии цензура не в состоянии. В условиях, когда социальные ресурсы стремительно развиваются, властям вряд ли удастся заделать все трещины в великой китайской *интернет-стене*.

ЗАКЛЮЧЕНИЕ

На основе анализа тенденций развития интернета в Китае и методов, используемых для обеспечения информационной безопасности, можно сделать вывод о том, что глобальная сеть в Поднебесной рассматривается как специфическая

инновационная среда, в рамках которой происходит формирование нового Китая и врастание его в мир. Для этого страна стремится максимально полно использовать экономические и пропагандистские возможности интернета и других интерактивных технологий.

Главным сторонником и двигателем китайского интернета является государство, и только оно определяет, какие опасности и возможности может таить в себе тотальная информатизация страны с населением, численность которого превышает 1 млрд человек. Властям крайне выгодно появление относительно дешевого средства массовой информации, достаточно мощного с точки зрения возможности воздействия на зарубежную аудиторию и в то же время вполне *управляемого*, чтобы ограничить обратное воздействие.

Отличительной чертой китайского интернета является четкая регламентация не только технических и организационных процедур, но и поведения пользователей в виртуальном пространстве. О свободе слова в Китае не принято говорить вообще, а интернет здесь является свободной зоной лишь теоретически. В действительности же пользователи имеют целый ряд обязанностей и вынуждены считаться с ограничениями, накладываемыми на использование сети контролирующими органами.

В интересах достижения лидирующих позиций на мировой арене Китай активно занимается разработкой киберсредств. Руководству КНР становится все сложнее показывать свое невежество и невиновность при проведении активной разведки радиоэлектронных средств и проникновении в киберпространство зарубежных государств. Эффективность китайских кибератак объясняется тесным сотрудничеством между правительственными структурами и хакерами.

Для расширения возможностей Китая в киберпространстве НОАК активно взаимодействует с коммерческими организациями и сферой образования, что способствует получению доступа к передовым исследованиям и технологиям, в том числе к телекоммуникационным системам военного и двойного назначения. Снижение зависимости от информационно-коммуникационных технологий Запада и развитие собственного инновационного потенциала рассматриваются как важные средства обеспечения кибербезопасности КНР.

Посредством широкого инвестирования в интернет-технологии, в частности нацеленного на стимулирование создания СМИ в интернете и развитие социальных сетей, Китай стремится сформировать позитивный имидж государства на международной арене и *смягчить* за счет создания эффекта *плюрализма мнений* негативное восприятие зарубежной аудиторией некоторых проблем внутриполитического развития страны. Вместе с тем, стремясь расширить информационные каналы, вещающие из Китая, власти страны стремятся контролировать воздействие зарубежных СМИ на китайскую аудиторию. Но в условиях, когда интернет-технологии продолжают активно развиваться и внедряются в жизнь китайского общества, властям становится все сложнее контролировать и фильтровать трафик и контент.

Примечания

[1] Сунь Цзы. Искусство войны. М.: София, 2010. С. 56–58.

[2] Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U.S.–China Economic and Security Review Commission by Northrop Grumman Corp. 2012, 7 марта,

http://http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (последнее посещение — 30 августа 2012 г.).

[3] Segal A. Is China a Paper Tiger in Cyberspace? Council on Foreign Relations. 2012, 8 февраля, http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/(последнее посещение — 30 августа 2012 г.).

[4] Там же.

[5] Глобальный отчет по информационным технологиям 2010–2011 гг. Всемирный экономический форум. 2012, 13 января, http://strategy.ru/the-report-on-information-technology-2010–2011/(последнее посещение — 30 августа 2012 г.).

[6] Дынкин А., Пантин В. Мирное столкновение. *Россия в Глобальной Политике*. 2012. № 1 (март-апрель).

[7] По расходам на НИОКР страна уже вышла на второе место в мире после США.

[8] Гуанкай С. Всеобъемлющая концепция национальной безопасности Китая. *Россия в Глобальной Политике*. 2009. № 3 (май-июнь); Lu Yongxiang. Science &Technology in China: A Roadmap to 2050. Chinese Academy of Science, 2010.

[9] Мальцев А. Китайский Интернет: как за каменной стеной. *Вебпланета: журнал для подключенных.* 2009, 3 июня, http://http://www.webplanet.ru/review/life/2008/06/11/china.html (последнее посещение — 30 августа 2012 г.).

[10] Интернет в Китае. Справка. *РИА Новости*. 2010, 13 января, http://ria.ru/world/20100113/204310750.html (последнее посещение — 30 августа 2012 г.).

[11] Число пользователей интернета в Китае превысило размеры населения США. *РИА Новости*. 2009, 26 июля, http://ria.ru/society/20090726/178669834.html (последнее посещение — 30 августа 2012 г.).

[12] Число пользователей интернета в Китае превысило полмиллиарда человек, больше двух миллионов сайтов. *Gazeta.ru*. 2012, 17 января, http://http://www.gazeta.ru/news/lenta/2012/01/17/n_2168345.shtml (последнее посещение — 30 августа 2012 г.).

[13] Мажаров И. Интернет в Китае. *Мир Интернет.* 2008, 2 февраля, http://abirus.ru/content/564/581/582/591.html (последнее посещение — 30 августа 2012 г.).

[14] Ball D. China's Cyber Warfare Capabilities. *Security Challenges*. 2011. Vol. 7, No. 2 (Winter), http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html (последнее посещение — 30 августа 2012 г.).

[15] Положение интернета в Китае. Пресс-канцелярия госсовета КНР. 2011, 1 февраля, http://russian.china.org.cn/government/archive/baipishu/txt/2011–02/01/content_21857458_8.htm (последнее посещение — 30 августа 2012 г.).

[16] Мажаров И. Цит. соч.

[17] Число пользователей интернета в Китае превысило размеры населения США. *РИА Новости*. 2009, 26 июля, http://ria.ru/society/20090726/178669834.html (последнее посещение — 30 августа 2012 г.).

[18] *China Telecom* — китайская государственная компания телекоммуникаций, создана в 2002 г. и занимается предоставлением комплексных информационных услуг, в частности фиксированной телефонной свяи, мобильной связи, подключением и использованием интернет-сети. Включена в рейтинг 500 самых крупных предприятий мира. Общий объем капитала компании составляет 632,2 млрд юаней, общий объем операционных доходов за весь год превысил 220 млрд юаней. В компании работают 670 тыс. сотрудников.

[19] *China Mobile* — китайская телекоммуникационная компания, создана в 1997 г. выделением из китайской государственной телекоммуникационной монополии *China Telecom*. Штабквартира компании расположена в Гонконге. Крупнейший в мире по количеству абонентов (493 млн по состоянию на 2009 г. и капитализации оператор сотовой связи. По состоянию на 2010 г. *China Mobile* контролировала около 70% китайского рынка.

[20] *China Unicom* — оператор связи в КНР. Компания основана в качестве государственной корпорации в 1994 г. Министерством промышленности и информационных технологий КНР. Предоставляет широкий выбор услуг, включая общенациональную сотовую GSM-сеть, международную и местную телефонную связь, обмен данными, услуги широкополосного доступа в интернет и IP-телефонии. На конец апреля 2008 г. компания имела 125 млн GSM-пользователей и 43 млн подписчиков. По состоянию на 2010 г. *China Unicom* контролировала около 20% китайского рынка.

[21] Ball D. China's Cyber Warfare Capabilities. *Security Challenges*. 2011. Vol. 7, No.2 (Winter), http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html (последнее посещение — 30 августа 2012 г.).

[22] *Магистральные узлы* (*backbone networks*) — общий термин для обозначения совокупности базовых узлов распределенной сети, соединенных высокоскоростными магистральными каналами. Сегменты сети масштаба предприятия, а также кластеры и отдельные станции подключаются к магистральной сети через мосты, маршрутизаторы и концентраторы. Особые требования предъявляются к надежности магистральной сети. Традиционная магистральная сеть называется распределенной, что подчеркивает ее отличие от локализованной и коммутирующей магистралей.

[23] *Firewall* (*файрвол*, синоним — *брандмауэр*) — компьютер, маршрутизатор или другое коммуникационное устройство, ограничивающее доступ к защищаемой сети и осуществляющий контроль и фильтрацию перехватываемых сетевых пакетов в соответствии с заданными правилами.

[24] Положение интернета в Китае.

[25] Мажаров И. Цит. соч.

[26] Положение Интернета в Китае.

[27] Тодрес В. Китай после *Google* — конец миссионерского капитализма? *TV. Net.UA.* 2010, 21 января, http://http://www.gzt.ru/column/283744.html (последнее посещение — 30 августа 2012 г.).

[28] Бывший аналитик Пентагона заявил, что Китай может перекрыть весь механизм телекоммуникации на оборудовании, которое было продано им в США. *Военно-политическое обозрение.* 2012, 13 июня, http://http://www.belvpo.com/12173.html (последнее посещение — 30 августа 2012 г.).

[29] *Northrop Grumman* — одна из наиболее высокотехнологичных компаний ВПК США, занимающаяся разработками в области электроники и информационных технологий, авиакосмической отрасли, судостроения и др. Кроме того, корпорация занимается разработкой перспективного вооружения для министерства обороны США, а также проведением исследований, направленных на совершенствование средств и методов защиты информации.

[30] Комиссия по американо-китайским отношениям в области экономики и безопасности *(The U.S.–China Economic and Security Review Commission)* была создана Конгрессом США в 2000 г. и получила полномочия вести мониторинг и расследования различных аспектов торгово-экономических и военных взаимоотношений с Китаем. Организация регулярно представляет доклады Конгрессу США, а также имеет возможность вырабатывать рекомендации по изменению законодательных и административных мер, влияющих на отношения между двумя странами.

[31] В Китае появились *кибервойска*. *Chip.Ru*. 2011, 31 мая, http://http://www.ichip.ru/mobile/novosti/sobytiya/2011/05/v-kitae-poyavilis-kiber-voiska/mobile_view (последнее посещение — 30 августа 2012 г.).

[32] Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U.S.–China Economic and Security Review Commission by Northrop Grumman Corp. 2012, 7 марта,

http://http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (последнее посещение — 30 августа 2012 г.).

[33] Юрченко Г. Возможности Китая по проведению компьютерных сетевых операций и кибершпионажу. *Военно-политическое обозрение*. 2012, 20 апреля, http://http://www.belvpo.com/9984.html (последнее посещение — 30 августа 2012 г.).

[34] Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U.S.–China Economic and Security Review Commission by Northrop Grumman Corp. 2012, 7 марта,

http://http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (последнее посещение — 30 августа 2012 г.).

[35] Черненко Е., Габуев А. Оружие к сбою. *Коммерсантъ.* 2011, 15 февраля. № 26 (4567), http://http://www.kommersant.ru/doc/1585823 (последнее посещение — 30 августа 2012 г.).

[36] Markoff J. Cyberattack on Google Said to Hit Password System. *The New York Times*. 2010, 19 апреля, http://http://www.nytimes.com/2010/04/20/technology/20google.html?_r=2 (последнее посещение — 30 августа 2012 г.).

[37] Юрченко Г. Возможности Китая по проведению компьютерных сетевых операций и кибершпионажу. *Военно-политическое Обозрение*. 2012, 20 апреля, http://http://www.belvpo.com/9984.html (последнее посещение — 30 августа 2012 г.).

[38] Другов А. Политическая культура. Массовое насилие в Индонезии: социальные, культурные и политические корни. *East View*. 2000, 11 января, http://dlib.eastview.com/browse/doc/2450717?enc=rus (последнее посещение — 30 августа 2012 г.).

[39] Габуев А. Желтая киберугроза. Китай готовится к войнам в киберсети. *Коммерсантъ-Online*. 2011, 15 февраля, http://http://www.kommersant.ru/doc/1585979 (последнее посещение — 30 августа 2012 г.).

[40] Подробнее см. в настоящем номере *Индекса Безопасности*: Якушев М. Интернет–2012 и международная политика. *Индекс Безопасности*. 2013. Весна. №1 (104). С. 29–42.

[41] Екатеринбургская декларация глав государств — членов Шанхайской организации сотрудничества. Президент России. Официальный сайт. 2009, 16 июня, http://archive.kremlin.ru/text/docs/2009/06/217868.shtml (последнее посещение — 30 августа 2012 г.).

[42] Декларация 10-го заседания Совета глав государств — членов Шанхайской организации сотрудничества. Центральный портал Шанхайской организации сотрудничества. 2010, 12 июня, http://http://www.infoshos.ru/ru/?id=74 (последнее посещение — 30 августа 2012 г.).

[43] DNS-расширение для автономного Интернета (AIP) — способ работы альтернативных корневых DNS-серверов в пределах национальных границ при помощи особых шлюзов.

[44] Китай предложил «расширить DNS для автономного интернета». *SecurityLab*. 2012, 21 июня, http://http://www.securitylab.ru/news/426071.php (последнее посещение — 30 августа 2012 г.).

[45] Евдокимов Е. Политика Китая в глобальном информационном пространстве. *Международные процессы.* 2011, январь–апрель. Т. 9, № 1 (25). http://http://www.intertrends.ru/twenty-fifth/009.htm (последнее посещение — 30 августа 2012 г.).

[46] Там же.

[47] Положение интернета в Китае.

[48] Тарасенко П. Интернет загородят великой стеной. *Коммерсантъ.* 2012, 30 мая. № 96 (4881). http://http://www.kommersant.ru/doc/1946451 (последнее посещение — 30 августа 2012 г.).

[49] Цой А. Китайские блогеры обходят цензуру. *Telecom Blog*. 2012, 26 марта, http://telecomblog.ru/?p=10702 (последнее посещение — 30 августа 2012 г.).

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ГЛОБАЛЬНОЕ УПРАВЛЕНИЕ ИНТЕРНЕТОМ: ВЗГЛЯД РОССИЙСКИХ И МЕЖДУНАРОДНЫХ ЭКСПЕРТОВ НА ВСТРЕЧЕ В ЖЕНЕВЕ

Первые 12 лет XXI в. были отмечены революционными изменениями в результате невероятно быстрого развития информационных и телекоммуникационных технологий (ИКТ), и в первую очередь интернета. Изменения затронули практически все пласты общественных процессов, включая международные отношения — от социальных и политических преобразований в арабском мире (Арабская весна) до беспрецедентного роста таких феноменов, как политически мотивированный хактивизм, слив государственных секретов в Сеть (Wikileaks), кибервойны и кибершпионаж. В то же время нарастает глобальная озабоченность вопросами предотвращения (либо победоносного ведения) войн в киберпространстве. Интернет и его эволюция не просто определяют все эти процессы, но и лежат в их основе. В связи с трансграничным характером глобальной сети последствия ее трансформации распространяются на всю планету. В процессе кардинальных преобразований сегодня находится вся архитектура глобального управления интернетом. Настоящая революция разворачивается и на третьем уровне интернет-архитектуры — на уровне пространства доменных имен DNS. Отдельным вопросом является регулирование транснациональных социальных сетей. Однако на данный момент ни один из этих вопросов не решается в рамках всеобщей, гармонизированной и всесторонней международной системы регулирования или хотя бы в рамках международного сотрудничества, способного закрыть все существующие пробелы и преодолеть проблемы, возникающие в данной области.

Анализ этих фундаментальных тенденций с использованием совместного и сбалансированного подхода всего международного сообщества требует широкого участия международных экспертов. Цели диалога состоят в выработке общих позиций в международном экспертном сообществе и формулировании совместной российской и европейской повестки дня по данным вопросам на неправительственном уровне. ПИР-Центр попытался положить начало подобному международному диалогу: 26 апреля 2012 г. в Женеве состоялось совместное расширенное заседание Международного клуба Триалог и европейского отделения ПИР-Центра, Centre russe d'etudes politiques.

*Заседание открыл президент ПИР-Центра Владимир **Орлов**. Главный доклад круглого стола был представлен председателем правления ПИР-Центра Михаилом **Якушевым**. В заседании участвовали: глава Программы по новым угрозам безопасности Института ООН по исследованию проблем разоружения Бен **Бейсли-***

***Уокер**, директор отделения общественной политики ISOC Констанс **Боммелер**, заместитель постоянного представителя Российской Федерации в ООН и других международных организациях в Женеве Виктор **Васильев**, профессор гражданского, коммерческого и европейского законодательства Цюрихского университета Рольф **Вебер**, вице-президент Международного Общества Интернет (ISOC) Маркус **Куммер**, советник по стратегическим и политическим вопросам Отдела корпоративной стратегии Международного союза электросвязи Ярослав **Пондер** и заместитель постоянного представителя США на Конференции по разоружению в Женеве Уолтер **Рид**.*

ВЛАДИМИР ОРЛОВ (ПИР-ЦЕНТР): ПИР-Центр развивает проект в области глобального управления интернетом и международной информационной безопасности, пытаясь обобщить и довести до наших партнеров видение этих проблем из России. Здесь существует большое количество проблемных областей, в том числе *облачные* компьютерные системы и их безопасность; идентификация в интернете; использование социальных сетей. Иногда у меня складывается впечатление, что мы рискуем утонуть в огромном потоке тем, сконцентрированных *под шапкой* нашего проекта. Конечно, существует множество юридических проблем — например, связанных с неучастием России в Будапештской конвенции *О киберпреступности* и в других *жестких* и *мягких* законодательных механизмах, направленных на эффективную борьбу с трансграничной киберпреступностью. В этой связи ПИР-Центр ставит перед собой задачу охватить все многочисленные грани этой проблематики, начиная с юридических и технических аспектов и заканчивая выработкой практических рекомендаций для лиц, принимающих решения в РФ, и их ключевых зарубежных партнеров.

В сферу интересов ПИР-Центра входит весь спектр данной проблематики, однако основное внимание уделяется, конечно же, вопросам, лежащим в плоскости практической политики. Как повлиять на политический курс? Как можно и необходимо скорректировать его, для того чтобы он отражал реальную ситуацию и учитывал текущие глобальные процессы? Именно на этих вопросах мы хотели сконцентрироваться, когда запускали наш проект.

А сейчас давайте приступим к самому первому заседанию в широком составе, которое в определенном смысле также является частью этого проекта. Я бы хотел, чтобы сегодня мы обсудили такие ключевые вопросы, как трансформация архитектуры интернета и системы управления Сетью; новая повестка дня в области международной информационной безопасности и ключевых проблем киберпространства и, конечно же, роль России во всех этих вопросах глобального порядка.

АРХИТЕКТУРА ИНТЕРНЕТА И УРОВНИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

МИХАИЛ ЯКУШЕВ (ПИР-ЦЕНТР): Прежде всего я бы хотел отметить различия в определениях и терминологии вопроса, который мы сейчас обсуждаем. В русском языке и российской дипломатии в основном используются термины, которые отличаются от широко распространенных на международном уровне понятий *управление интернетом* [*internet governance*] и *кибербезопасность* [*cyber security*]. Вместо этого Россия развивает и продвигает концепцию *информационной безопасности* [*information security*] — в нашей стране наиболее широко используется именно этот термин. Фактически мы говорим об одних и тех же явлениях и проблемах, однако обозначаем их разными словами, поэтому нам следует попытаться понять друг друга и постараться говорить на одном языке.

Управление интернетом имеет множество разных аспектов, и в этом смысле оно не отличается от любого другого комплексного аспекта международной безопасности. Когда мы ведем речь об освоении космоса и связанных с ним юридических

и политических вопросах, нам следует принимать во внимание принципы космической деятельности, включая принцип ответственности, прав и обязанностей запускающих космические аппараты государств, правовой статус Луны и других небесных тел и т.д. Когда мы говорим об атомной энергии, нам нужно иметь в виду проблемы контроля над вооружениями, нераспространения, военного и мирного использования ядерных материалов, ответственность ядерных операторов и другие подобные вопросы. То же самое относится и к интернету — невозможно дать короткие и точные ответы на вопросы о том, что делать в сфере управления интернетом, кто несет ответственность за это управление и какие договоры или конвенции следует разработать, чтобы закрыть пробелы и найти решение всем существующим проблемам.

Более того, когда заходит разговор об интернете, мы иногда говорим об абсолютно разных вещах, которые в своей совокупности образуют понятие «интернет». Сюда входит техническая инфраструктура, каналы телекоммуникаций и различные типы оборудования, которые обеспечивают доступ к сети. Сетевая инфраструктура радикально отличается от той системы, которую мы имели в эпоху *традиционных* телекоммуникаций, таких как телеграф или телефон. Наконец, говоря об уровне практического использования интернета, следует учитывать, какую важность приобрела глобальная сеть, особенно в связи с колоссальными достижениями в ее развитии и проникновении в мире.

Однако даже на уровне инфраструктуры существуют различные подуровни, которые регулируются различными организациями в соответствии с самыми разными принципами. В понятие инфраструктуры Сети входят волоконно-оптические кабели, спутниковые каналы, радиочастотный спектр и т.д. Сюда же относятся такие вопросы, как так называемые *проблемы последней мили*, а также различные типы оборудования для доступа, пользовательского оборудования и оборудования на площадке клиента интернет-сервисов. В данной сфере применяются совершенно другие принципы регулирования, если речь идет, например, о станциях спутниковой связи.

То же можно сказать и о самой сетевой архитектуре, которая весьма разнообразна в техническом, организационном и регуляторном плане. Говоря о сетевой архитектуре, следует учитывать различные ее уровни, начиная с уровня корневых серверов — речь идет о знаменитых корневых серверах, которые расположены в разных странах мира; они представляют собой *ядро* интернета. Нужно также учитывать вопросы, связанные с развитием системы IP-адресации: в настоящий момент мы наблюдаем переход с предыдущей версии IP-протокола, *IPv4*, на новую версию, *IPv6*. Этот переход будет означать значительное изменение всей архитектуры интернета. Фактически интернет превращается из *сети людей* в *сеть предметов* — собственные IP-адреса смогут получить — и уже получают — наши холодильники, автомобили и различные электронные устройства, приобретающие способность обмениваться информацией.

Третьим уровнем сетевой архитектуры является система доменных имен, которая связана с геополитикой. К настоящему моменту сложилась система так называемых доменов верхнего уровня, соответствующих коду страны и определенным образом отражающих принцип государственного суверенитета. Однако в 2012 г. начали внедряться нововведения, согласно которым количество доменов верхнего уровня увеличивается до нескольких сотен или даже тысяч. Например, становятся возможным такие домены верхнего уровня, как *.microsoft*, *.Facebook*, *.google*, *.religion*, *.luckilyman,* то есть благодаря этому гениальному нововведению становится возможным создать и ввести в использование практически любое доменное имя. Многие обыватели, управленцы и даже эксперты пока не понимают, сколь масштабные изменения предстоят в этой связи в ближайшее время и как эти изменения отразятся на всех нас.

Наконец, на уровне практических приложений существует огромное количество вебсайтов. Их число уже исчисляется миллиардами; они регулируются различными способами и по законодательству разных юрисдикций, но с помощью них мы понимаем, что происходит в интернете — и это именно то, для этого существует и используется интернет. Однако сам по себе вебсайт должен регулироваться, так же, как это происходит со средствами массовой информации. В разных странах СМИ регулируются независимо от того, являются ли они онлайновыми или оффлайновыми, и это очень важный вопрос в контексте распространения информации и развития массовых коммуникаций. Скоро уже не будет проблемой найти в интернете любую информацию, вовсе не используя систему доменных имен. Это можно сделать с помощью таких поисковиков, как *Google* или *Yandex*. К примеру, если вы хотите узнать, что такое *Centre russe d'etudes politiques*, который является организатором нашей сегодняшней встречи, совсем не обязательно запоминать название этой организации в швейцарском домене *.ch*. Достаточно ввести его или название любой другой организации в поисковик, и с вероятностью 100 % поисковая машина выведет вас на нужный интернет-ресурс. При этом не играет никакой роли, где именно данный ресурс расположен.

Особенно большие возможности в сегодняшнем интернете предлагают социальные сети, в частности потому, что практически никак не регулируются. Большинство социальных сетей транснациональны, а их аудиторию составляют *юзеры* со всего мира. Количество пользователей *Facebook* недавно перевалило за 900 млн человек. Если бы аудитория сети Марка Цукерберга составляла население одной страны, то эта страна была бы третьей в мире по численности населения после Китая и Индии. Соответственно, возникают вопросы о том, кто должен регулировать деятельность пользователей *Facebook* и с какой регулирующей инстанцией должна взаимодействовать данная социальная сеть по вопросам, так или иначе затрагивающим проблематику обеспечения глобальной безопасности.

Еще одно новое измерение, которое сейчас активно развивается — это мобильное пространство интернет-коммуникации. Во многих странах — и Россия здесь не исключение — многие пользователи все чаще выходят в интернет не через традиционные компьютеры, а со своих мобильных телефонов, планшетов и других портативных устройств. Это тоже очень сильно меняет ландшафт интернета, поскольку уже сейчас есть некоторые приложения, которые не работают на обычном настольном компьютере — они адаптированы именно под портативные устройства. Поэтому нам также необходимо говорить об интеграции мобильных сетей и компьютерных сетей в интернете. В 2020 г. интернет будет сильно отличаться от сегодняшней глобальной сети, точно так же, как сегодняшний интернет сильно отличается от интернета пятнадцатилетней или даже десятилетней давности.

РОЛЬФ ВЕБЕР (ЦЮРИХСКИЙ УНИВЕРСИТЕТ): Относительно важности инфраструктуры ни у кого сомнений нет. Мы также понимаем, что сегодня дело приходится иметь с самой разнообразной инфраструктурой. Одного лишь анализа телекоммуникационных сетей для рассмотрения проблемы мало — нужно учитывать спутники, радиочастотный спектр, а также постоянно растущее количество мобильных телефонов. Что касается России, то, как уже сказал М. В. Якушев, в этой стране использование мобильных телефонов для доступа в интернет широко распространено, как и во многих других странах мира. Мне часто приходится работать в Восточной Азии, и во многих странах этого региона основным способом доступа в интернет уже стал именно мобильный телефон, а не компьютерные сети. Новые технологии также направлены на разрешение вопросов безопасности, и нам это следует учитывать.

Основным прародителем нынешней глобальной сети было американское Министерство обороны, то есть американские военные. Давайте вспомним сеть ARPANET, которая с течением времени все больше и больше развивалась в сто-

рону обслуживания гражданского и частного сектора с одновременным сокращением роли военных. Сегодня мне иногда даже кажется удивительным, что чем больше дискуссия сводится к вопросам обороны и безопасности, тем менее важной она начинает казаться в контексте общей проблематики развития интернета. Дискуссии на эту тему уже не представляются настолько значимыми, как в самом начале эпохи Сети, когда сам интернет и его техническая инфраструктура только начинали формироваться в обстановке холодной войны.

ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ И УПРАВЛЕНИЕ ИНТЕРНЕТОМ

ЯКУШЕВ: Очень интересные дебаты разворачиваются сегодня вокруг принципа суверенитета государств. Сохраняет ли государство свой суверенитет в эпоху интернета или же концепция политического суверенитета трансформируется, размывается, превращаясь, к примеру, в концепцию *совместного суверенитета*? На этот вопрос очень трудно дать однозначный ответ. С одной стороны, существует широкое международное признание недопустимости вмешательства во внутренние дела любой страны. Никто не оспаривает право Китая, Ирана или арабских стран накладывать определенные ограничения на интернет, на доступ в интернет, или на распространение информации в Сети в пределах своей страны.

Однако есть также пример Ливии и Сирии, в ситуации с которыми со стороны международного сообщества и отдельных стран проявляют себя так называемые интересы гуманитарного вмешательства. Массовые нарушения прав человека в этих странах используются как предлог определенными странами или международными организациями, которые хотят изменить ситуацию и стремятся прекратить нарушения прав человека теми или иными способами. Появляются различные международные либо национальные документы, имеющие международные последствия, такие как, например, Международная стратегия по действиям в киберпространстве (2011 г.), которая излагает и фиксирует принципы поведения США в киберпространстве. Этот документ спровоцировал горячие дебаты по всему миру. Есть и предложения Российской Федерации, на которых я подробно остановлюсь чуть позднее. Однако на сегодняшний день, к сожалению, несмотря на ведущиеся дискуссии в рамках ООН, мы не видим перспектив для компромисса. К сожалению, вопросы, связанные с обеспечением международной информационной безопасности (МИБ) и глобальным управлением интернетом, в массе своей крайне политизированы. *Арабская весна* и революционные события в разных странах на фоне активной социальной самоорганизации в социальных сетях, ограничения на свободу слова и другие политически *чувствительные* процессы не дают нам возможности говорить о разработке документа, а точнее, международного юридического инструмента, который заполнил бы существующие пробелы и дал ответы на все эти вопросы. Однако в то же время вполне очевиден ряд проблем, в скорейшем разрешении которых заинтересованы все, с другой стороны, нет времени ждать, пока эти проблемы каким-то образом разрешатся сами собой.

Я бы хотел привлечь ваше внимание к решению, принятому Советом Европы, который объединяет почти все страны европейского континента и к чьим документам относятся с уважением не только в европейских странах, но и по другую сторону Атлантики — в Америке, Африке, в азиатских странах. В прошлом году, 21 сентября 2011 г., Комитет министров Совета Европы принял ряд очень важных документов, которые следует рассматривать в качестве элемента так называемого *мягкого права в области информационной безопасности*. Речь не идет о международном договоре или резолюции Совета Безопасности ООН, имеющих обязательную юридическую силу. Но поскольку Россия и большинство стран Европы являются членами Совета Европы, такие рекомендации и *мягкие* законодательные документы являются отличным примером возможного компромисса по определенным вопросам,

относящимся к управлению интернетом. Речь идет, в частности, о трансграничном ущербе и трансграничных последствиях действий государств. В этой связи Совет Европы принял декларацию Комитета министров о принципах управления интернетом, в которой были одобрены рекомендации для государств — членов СЕ в области защиты и развития всеобщего, целостного и открытого характера интернета.

Существует 10 принципов управления интернетом, общепринятых для всех европейских страна, включая страны — члены Совета Европы. К числу таких принципов относится, в частности, защита фундаментальных прав и свобод, а также повсеместное укоренение *мультистейкхолдерской модели* управления интернетом, то есть модели, предполагающей участие в процессе управления всех заинтересованных сторон.

Существует также принцип ответственности государств. Управление интернетом очень часто затрагивает права государств, и в этом смысле Совет Европы создал прецедент, установив принцип ответственности за предотвращение нанесения трансграничного ущерба — в том числе ущерба вследствие принятия определенных внутригосударственных законов и правил. Известен ряд примеров, когда внутренние решения или даже непреднамеренные действия на уровне одних государств наносили определенный ущерб другим государствам. К примеру, в 2011 г. одна женщина в Грузии умудрилась перерубить лопатой оптико-волоконный кабель, проходящий через ее деревню. В результате без доступа к Сети осталась вся Армения.

Что нужно сделать, чтобы не допустить повторения таких инцидентов? Я не собираюсь перечислять все 10 принципов, но некоторые из них все же стоит упомянуть. Девятый принцип гласит, что нельзя допускать никакого манипулирования интернет-трафиком. К примеру, нельзя наделять приоритетом определенные виды трафика. Кроме того, нельзя ограничивать доступ к определенным типам ресурсов по политическим или иным причинам, если такие меры не соответствуют требованиям международного законодательства по защите свободы слова и свободы доступа к информации. Очень важен десятый принцип — принцип культурного и языкового разнообразия, распространяющийся на виртуальное пространство глобальной сети.

Предпринимались неоднократные попытки выработать международный документ, который ответил хотя бы на некоторые открытые вопросы. В 2005 г. бывший генеральный секретарь ООН Кофи Аннан организовал в Женеве несколько заседаний Рабочей группы по управлению интернетом. Все члены рабочей группы были назначены самим генеральным секретарем. Окончательный отчет группы был опубликован в 2005 г. и содержал определенные конкретные решения, пояснения и параграфы, в рамках которых действительно была предпринята попытка дать ответ на некоторые из приоритетных вопросов в области глобального управления интернетом. Темы, затронутые в этом отчете, в настоящее время обсуждаются на заседаниях Форумов по управлению интернетом, которые проводятся ежегодно.

В других предложениях, вносимых такими странами, как США и Россия, фундаментальные принципы международного права должны стать неотъемлемой частью — иначе будет очень трудно защищать и продвигать на глобальной арене их основные идеи и положения. К примеру, если мы пытаемся предотвратить *кибервойну*, нужно одновременно работать над предотвращением незаконной деятельности интернет-пользователей, направленной против государства и общества (кибертерроризм), а также незаконные действия против других пользователей (т.е. киберпреступность). Стоит также вопрос о предотвращении незаконных действий правительств и группировок, действующих в их интересах, против интернет-пользователей.

ВЕБЕР: Конечно, один из ключевых вопросов — насколько и в какой степени нам вообще необходимо регулирование интернета. В самом начале, в 1996 г., Джон Перри Барлоу заявил в своей знаменитой Декларации независимости киберпространства, что нам вообще не нужно никакое регулирование, поскольку киберпространство является абсолютно отдельным миром, которому не нужны указки правительства или игроков частного сектора. Естественно, с тех пор взгляды на вопрос регулирования очень сильно изменились. Этот процесс привел, как очень хорошо и подробно нам рассказал М. В. Якушев, к появлению идеи управления интернетом с силами множества стейкхолдеров, то есть заинтересованных участников. У нас сейчас есть три основных столпа: правительства, частный сектор и гражданское общество. Однако существует и такой феномен: частный сектор и гражданское общество все больше концентрируются на таких аспектах, как система доменных имен, защита личной информации, права человека и цензура, несколько дистанцируясь от вопросов безопасности киберпространства.

Если посмотреть на список тем, обсуждаемых на Форумах по управлению интернетом (IGF) за последние шесть лет, становится очевидно, что вопросам кибертерроризма и киберпреступности, к примеру, уделяется очень мало внимания. Я не говорю, что эти вопросы вообще не обсуждаются, но нет сомнений, что такие дискуссии находятся на периферии внимания в рамках Форума IGF — по крайней мере, именно так обстояли дела на первых пяти форумах. Это на самом деле не так уж и удивительно, поскольку проблемы кибертерроризма и особенно кибервойн в основном решаются на уровне правительств, в то время как участники IGF в большей степени представляют гражданское общество. Так что, наверное, для участников этих форумов киберпреступность играет определенную роль, но намного больше их заботят другие проблемы. Именно поэтому, к примеру, обсуждение Конвенции Совета Европы *О киберпреступности* так долго не включалось в повестку дня IGF. При этом на заседаниях Корпорации по присвоению имен и номеров в интернете (ICANN) аспекты киберпреступности и кибербезопасности вообще не играли и до сих пор почти не играют никакой роли. Вместе с тем, международное сообщество, похоже, движется в направлении определенного компромисса. М. В. Якушев упомянул попытку Совета Европы решить вопрос о закреплении принципов управления интернетом. Правительства некоторых других стран — к примеру, Бразилии — также начали работу над формулированием принципов управления глобальной сетью. Предпринимаются попытки выработать что-то вроде *декларации о правах человека в интернете*. Подобная инициатива в настоящее время поддерживается компанией *Google* через один исследовательский институт в Берлине, которому с этой целью предоставляются довольно серьезные ресурсы.

Однако, как это ни удивительно, я пока не вижу особого внимания к вопросам национальной или международной безопасности в контексте киберпространства и в частности интернета. По моему мнению, эта сфера требует более пристального внимания. Решать эту проблему нужно уже в ближайшем будущем — более того, я бы даже сказал, что ее нужно решать срочно, пока не стало слишком поздно. Иными словами, акцент необходимо делать на мерах безопасности. Наконец, хотелось бы также упомянуть, что уже есть пара документов в этой области, которые можно использовать в качестве основы для дальнейшего обсуждения. К примеру, Организация экономического сотрудничества и развития (ОЭСР), которая хотя и не является всемирной организацией, но объединяет 34 государства в основном из числа развитых стран, в 2002 г. опубликовала свои рекомендации по информационной безопасности. Таким образом, опыт практических наработок ОЭСР в этой сфере насчитывает уже 10 лет и вполне может быть использован в качестве отправной посылки для дальнейшего обсуждения.

КОНСТАНС БОММЕЛЕР (**INTERNET SOCIETY**): Я бы хотела добавить несколько слов к тому, что сказал профессор Вебер. На международном уровне уже сейчас предпринимаются определенные усилия в области борьбы с киберпреступностью

и обеспечения безопасности киберпространства. Недавно Интерпол объявил о своей работе над созданием глобальной системы, которая позволит быстро идентифицировать авторов незаконных действий в киберпространстве. Я не знаю, насколько широко известны эти инициативы, но мне представляется, что первые определенные шаги в плане международного сотрудничества уже делаются. Конечно, работая над этими инициативами, нужно не забывать о нерешенных вопросах в плане неприкосновенности личной жизни и персональных данных, так что продвигаться в этом направлении следует осторожно. Но определенные усилия уже предпринимаются, и мы будем надеяться, что они дадут положительный результат.

ВЕБЕР: Я бы хотел прокомментировать по крайней мере пару заявлений и мыслей, высказанных М. В. Якушевым. Наверное, стоит начать с вопроса о том, как вообще подходить к проблеме регулирования интернета. Есть ли какая-то реальная необходимость в таком регулировании? Кто должен устанавливать правила? Чьи интересы должны быть защищены этими правилами, и нужны ли какие-то специальные механизмы? Если проанализировать последние 15 лет с тех пор, как была создана ICANN, то становится ясно, что теперь в управлении киберпространством принимает участие широкое сообщество и что это привело к очень интересным изменениям. Фактически произошел переход от централизованного регулирования к интересам отдельных государств и мультистейкхолдерской модели.

Кроме того, возвращаясь к темам, которые я уже затрагивал, я также считаю, что существует необходимость в усовершенствовании структуры ICANN. Что касается заявок на новую систему доменных имен DNS, в этой связи была зафиксирована серьезная проблема с безопасностью. Судя по всему, лица, подавшие заявки, могли получить несанкционированный доступ к информации, принадлежащей другим заявителям, которые уже загрузили свою информацию. Реакция ICANN на эту ситуацию была, на мой взгляд, недостаточно профессиональной. Фактически, представители ICANN лишь заявили, что делают все возможное для решения этой проблемы с безопасностью. Однако не последовало никаких четких рекомендаций относительно того, какие действия нужно было предпринимать. Осталось непонятно, кто отвечает за сложившуюся ситуацию в самой Корпорации. Отсутствовало даже четкое разделение сфер ответственности и, наконец, было невозможно применить правила об ответственности за ущерб, поскольку непонятно было, какой конкретно ущерб был нанесен в связи с утечкой информации. Описанная выше ситуация подтвердила потребность детально проанализировать глобальные аспекты безопасности интернета в рамках ICANN.

Мое предположение в этой связи сводилось к тому, что необходимо заложить прочную институциональную основу для управления ICANN, поскольку вопросы легитимности больше невозможно игнорировать. Я подал некоторые предложения относительно возможных путей устранения слабых мест в существующей системе. Я не говорю, что нужно искать замену Корпорации как таковой. Но я полагаю, что ICANN должна в большей степени учитывать широкие общественные интересы. И как специалист в области права, я не могу не отметить, что в настоящее время не существует даже нормальной системы для подачи апелляций на решения и действия Корпорации. Структура, которая необходима для придания баланса существующей системе, не должна представлять собой судебную инстанцию. Тем не менее существует явная потребность в некоем независимом органе для рассмотрения решений, принимаемых ICANN.

ЯРОСЛАВ ПОНДЕР (МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ): Кибербезопасность является ключевым компонентом Женевского плана действий и Тунисской повестки дня, которые предлагают механизм имплементации. МСЭ предпринимает необходимые меры, чтобы Глобальная программа в области кибербезопасности, вступившая в силу в 2007 г. с участием всех ключевых сообществ

стейкхолдеров, принесла желаемые плоды на глобальном уровне. Эта дискуссия также получила развитие на Всемирном саммите по информационной безопасности, который состоялся 14–18 мая 2012 г. Мы вступили в фазу подведения промежуточных итогов этих процессов и анализируем результаты саммита. На этой основе мы стараемся понять, что хотели бы увидеть государства-участники после 2015 г. в плане глобальных мероприятий и с какими ранее неизвестными факторами и проблемами мы можем столкнуться. Поэтому вклад со стороны сообщества стейкхолдеров имеет огромное значение для разрешения многих вопросов, которые упоминались сегодня в ходе дискуссии и стали предметом обсуждения на ряде сессий в ходе Всемирного саммита.

Форум — не просто площадка для дискуссий, он ставит своей целью практическое воплощение принятых решений. Слушая сегодняшнюю дискуссию, я рад слышать конкретные предложения, созвучные тем сюжетам, которые стали предметом обсуждения на Всемирном саммите. Глобальная программа в области кибербезопасности (ГПК) предлагает рамочную основу, однако много времени и сил уделяется текущей работе с различными странами, чтобы обеспечить глобальное реагирование на национальные, региональные и глобальные киберугрозы и чтобы ни один человек не боялся выйти в интернет со своего мобильного телефона или компьютера. Одним особо важным направлением в этой широкой рамочной нише является Международное многостороннее партнерство против киберугроз (ИМПАКТ). Более 140 стран уже присоединились к этой глобальной инициативе, а некоторые государства получают от МСЭ помощь в создании на национальном уровне групп и центров реагирования на компьютерные инциденты. Иногда такие центры приходится создавать с нуля, и мы рады, что так много стран готовы поставить этот вопрос во главе повестки дня. Я думаю, наступил момент объединить наши усилия и обсудить сотрудничество в рамках ГПК на всех уровнях — как на высшем официальном, так и на оперативном. Это позволит обеспечить эффективность глобального реагирования на вызовы безопасности киберпространства.

МУЛЬТИСТЕЙКХОЛДЕРСКАЯ МОДЕЛЬ В УПРАВЛЕНИИ ИНТЕРНЕТОМ

ЯКУШЕВ: Наиболее важным вопросом, который освещается в окончательном докладе Рабочей группы по управлению интернетом, является необходимость укоренения подхода, уже упомянутого мной в связи с решениями Совета Европы. Речь идет о необходимости привлекать и обеспечивать равное участие всех основных групп заинтересованных участников, или, используя прижившийся англицизм, *стейкхолдеров* [stakeholders]. Значение термина *stakeholder* очень трудно без искажения смысла перевести на русский. Наиболее устоявшийся вариант перевода — «*заинтересованные участники».* В исходном, классическом варианте концепция мультистейкхолдеризма предполагала включение в процесс управления интернетом трех групп заинтересованных участников: правительств, частного сектора и гражданского общества. По мере того как концепция развивается, углубляется и наполняется практическим содержанием, к ним добавляются и другие сообщества. В итоге на сегодняшний день насчитывается уже пять категорий таких заинтересованных участников, или стейкхолдеров:

- правительства;
- частный сектор;
- гражданское общество;
- техническое сообщество;
- сами пользователи интернета как отдельное сообщество.

Неизменным остается то, что все участники должны сыграть одинаково важную роль. Это фундаментальный принцип, который должен учитываться при обсуждении будущего развития регулирования и управления интернетом, поскольку особая природа глобальной сети уже сейчас объединяет миллионы и миллиарды пользователей. Нам нужно использовать знания, опыт и возможности не только суверенных государств, но и частного сектора, компаний, которые разрабатывают технические стандарты интернета, и гражданского общества, заинтересованного в целом ряде вопросов, включая права человека, права потребителей и т.д. На сегодняшний день уже сложилась достаточно разветвленная система организаций, участвующих в управлении интернетом на международной уровне. Их список включает среди прочих Международный союз электросвязи (МСЭ) и ICANN. Что касается последней, то вряд ли ее можно охарактеризовать как международную или общественную организацию. Это некоммерческая корпорация со штаб-квартирой в Калифорнии, однако ее деятельность имеет глобальный масштаб. Именно ICANN вводит в эксплуатацию новые домены верхнего уровня и регулирует критически важные аспекты управления интернетом.

Существует ряд общих проблем, которые требуют совместного решения и сотрудничества. Во-первых, участие всех стейкхолдеров незаменимо во всех аспектах разработки и внедрения правовых норм в области управления интернетом и информационной безопасности. Мы наблюдаем аналогичную ситуацию в области освоения космоса, а возможно, даже в участии частных компаний в развитии атомной энергетики и эксплуатации источников атомной энергии. Поэтому участие всех заинтересованных сторон в управлении интернетом является обязательным условием дальнейшего успешного развития глобальной сети.

МАРКУС КУММЕР (**INTERNET SOCIETY**): Мне было очень приятно и интересно увидеть такой выраженный акцент на сотрудничестве с участием всех стейкхолдеров — мы в Обществе Интернета уверены в необходимости и правильности именно такого подхода. Однако я бы хотел сделать одну поправку или дополнение: в ходе нашей дискуссии зачастую звучит тезис о трех группах стейкхолдеров, однако на Всемирном саммите информационного общества в Тунисе мы добавили четвертую группу — представителей академического и технического сообществ. ISOC считает себя частью академического и технического сообщества и ассоциирует себя именно с этой группой заинтересованных участников процесса глобального управления интернетом. Кроме того, как уже ранее справедливо отметил М. В. Якушев, сегодня выделяется и пятая группа стейкхолдеров — непосредственно сообщество интернет-пользователей, чьи интересы также нельзя не учитывать.

БЕН БЕЙСЛИ-УОКЕР (ИНСТИТУТ ООН ПО ИССЛЕДОВАНИЮ ПРОБЛЕМ РАЗОРУЖЕНИЯ): Я бы хотел прокомментировать несколько моментов, так или иначе затронутых коллегами. Мне очень нравится идея участия в управлении глобальной сетью всего сообщества стейкхолдеров. Мои коллеги считают полезными мероприятия, на которых происходит обсуждение глобальной роли киберпространства и ведется поиск решений того, как мы собираемся этим пространством управлять и как мы будем формулировать политику в отношении интернета на национальном и международном уровнях. Однако мне кажется, что когда представители бизнеса, академического сообщества, а также лица, ответственные за выработку политического курса и принятие решений, собираются в одной аудитории, в 99 % случаев любое мероприятие распадается на три весьма интересные и насыщенные, но отдельные и невзаимосвязанные дискуссии. Между этими группами стейкхолдеров крайне редко наблюдается действительно эффективный диалог, особенно когда речь идет о тех пластах проблематики, с которыми работаю я в рамках Института ООН по исследованию проблем разоружения (ЮНИДИР), а также г-н Васильев в рамках своего ведомства, то есть

о роли киберпространства в контексте международной безопасности и глобальной политической динамики в этой сфере.

Мне также кажется, что международное сообщество профессионалов, занимающихся вопросами безопасности, особенно на дипломатическом уровне, не привыкло работать с неправительственным сектором и с бизнесом. Когда речь идет о ядерном оружии, нет такой острой потребности в участии негосударственных игроков в процессе переговоров и установлении нового режима, однако ситуация абсолютно противоположна, когда речь заходит о вопросах МИБ и глобального управления Сетью. Важно подчеркнуть, какая значительная часть интернета и его технической инфраструктуры сосредоточена в частных руках. У нас нет реально действующих механизмов, которые бы позволили нам пригласить людей, выросших в Силиконовой долине и привыкших крайне подозрительно относиться к правительству, на встречу с дипломатами и сказать им: давайте все вместе подумаем, как нам решить проблему. Этот момент следует учитывать и понимать его возможные последствия.

ВЕБЕР: Я бы хотел еще раз вернуться к идее участия всего сообщества стейкхолдеров в управлении интернетом. Мне кажется, эта идея совсем не означает, что можно обойтись вообще безо всякой рамочной правовой основы. Нам необходима система, которая в правовом плане является стабильной и устойчивой — я сейчас пользуюсь терминами, которыми обычно оперируют технические специалисты. Скорее всего, единственным источником, к которому мы можем обратиться за какими-то правовыми принципами, является международное *обычное* право. В этой области у нас также есть некоторые принципы, сформулированные Обществом Интернета (ISOC) и общепринятые в широком правовом сообществе.

М. В. Якушев в своей реплике упомянул договор о космосе. Это многосторонний документ, однако содержащиеся в нем ключевые принципы могут с успехом применяться и в других сферах. К примеру, у нас есть определенные законы, которые регулируют международное судоходство. Существуют и действуют законы о реках. В течение уже более 100 лет общепринято, что сторона, находящаяся у истока реки, не имеет права сбрасывать в нее опасные химикаты, поскольку это нанесет ущерб стороне, расположенной ниже по течению. Так что, скорее всего, при разработке будущих законопроектов в области национальной безопасности нам придется анализировать существующие принципы международного права, включая международное обычное право, чтобы понять, какие принципы являются общепринятыми.

В международном праве присутствует более или менее общепринятый принцип о недопущении трансграничного ущерба — превентивный принцип, зафиксированный в Декларации по окружающей среде и развитию, принятой в Рио-де-Жанейро в 1992 г., а также в некоторых документах Совета Европы и других международных организаций. Отталкиваясь от подобных принципов, мы могли бы попытаться положить начало дальнейшему обсуждению, которое неизбежно должно затронуть следующие вопросы: какие принципы могут получить дальнейшее развитие и что из них могло бы стать частью какого-то нового международного документа? Скорее всего, речь не будет идти о новом юридически обязывающем международном договоре: я не очень верю, что правительствам стран по всему миру удастся достичь согласия относительно такого документа. Но можно подумать о новых инструментах мягкого права, таких, например, как кодифицированные принципы и правила поведения.

УОЛТЕР РИД (ПОСТОЯННОЕ ПРЕДСТАВИТЕЛЬСТВО США НА КОНФЕРЕНЦИИ ПО РАЗОРУЖЕНИЮ В ЖЕНЕВЕ): В ходе обсуждений и переговоров о мерах по укреплению доверия с Россией и некоторыми другими государствами — вне зависимости от того, было ли у нас абсолютно согласованное правовое определе-

ние этого термина — часто обнаруживалось, что никакого готового определения вообще не существует. Меры, которые мы можем предпринять в сфере безопасности киберпространства, часто возможны только благодаря партнерству между государственными и негосударственными игроками. Г-н Якушев с этим, очевидно, тоже столкнулся. В США ситуация в области регулирования киберпространства именно такова: очень многие меры невозможны без сотрудничества с частным сектором, с негосударственными стейкхолдерами, которые привлекаются на основе добровольного сотрудничества. Поиск решений существующих проблем требует именно такого типа сотрудничества. Я думаю, такая ситуация станет нормой в течение следующих 10–15, максимум 20 лет, и именно в направлении развития модели мультистейкхолдеризма будет вестись основная работа. Учитывая абсолютную необходимость участия множества стейкхолдеров — это вполне здоровая ситуация, и очень хорошо, что правительства регулярно получают об этом напоминания. Так что мы считаем очень важным обсуждение этих вопросов на международном уровне, особенно в контексте проблем международной безопасности. Я благодарен ПИР-Центру за то, что он выводит эту дискуссию на уровень российско-американского гражданского сообщества, и считаю это очень важным шагом.

ОРЛОВ: Большое спасибо, г-н Рид. Пару недель назад к нам в Москву приезжала заместитель государственного секретаря США Роуз Готтемюллер. Конечно, к ней выстроилась очередь, чтобы поговорить об Иране или проблемах противоракетной обороны (ПРО), однако она начала разговор с вопроса о том, как информационные технологии могут изменить мир в сфере контроля над вооружениями и во многих других сферах. У нас состоялось оживленная и продуктивная беседа, которая продемонстрировала, что мышление в американской администрации действительно вышло на весьма высокий уровень, и это нас очень вдохновляет.

РИД: Тем, кто работает здесь, в Швейцарии, наверное, известно о проекте MELANI (Центр сбора и анализа информации). Это программа партнерства между государством и частным сектором, причем в данном случае речь идет о партнерстве между полицией и частным бизнес-сообществом. Это партнерский проект, который создает безопасное пространство между полицейским сообществом и теми сегментами бизнес-сообщества, наиболее подверженными киберпреступности и незаконным действиям в киберпространстве. Данный проект, скорее всего, не поможет исправить уже случившееся — я имею в виду ущерб, понесенный бизнесом от уже совершенных актов киберпреступности, но он поможет лучше понять, что происходит и как себя защитить в дальнейшем, поможет стать частью широкого сообщества пользователей. В проекте сочетаются элементы как государственного, так и частного участия, так что речь не идет об официальном государственном проекте. Деятельность MELANI помогает интернет-пользователям предотвратить повторение подобных ситуаций в будущем, и эта работа ведется на уровне провинций, а также на уровне муниципалитетов во многих странах по всему миру. Что-то подобное появляется в США, в Канаде — обычно на муниципальном, субнациональном уровне. В Швейцарии этот проект пока имеет экспериментальный статус, но такой пример может быть полезен и другим государствам, в том числе России.

РОССИЯ И ЕЕ МЕСТО В РЕГУЛИРОВАНИИ МИБ И УПРАВЛЕНИИ ИНТЕРНЕТОМ

ЯКУШЕВ: Хотелось бы сказать несколько слов о позиции России в области глобального регулирования информационного пространства и обеспечения МИБ, о том, какие предложения выдвигаются российской стороной и какие есть воз-

можности для сотрудничества, а также сделать некоторые выводы, которые можно будет обсудить в ходе нашей дискуссии.

К сожалению, у моей страны, как это принято считать, в основном за рубежом, — *плохая кредитная история*. Речь идет о распространенном мнении, что с учетом якобы практикуемой цензуры и политических ограничений на свободу общения в интернете Россия находится не в том положении, чтобы вносить какие-либо предложения в международную повестку или проявлять какую-то активность в сфере МИБ и управления интернетом. Кибератаки против Эстонии, Грузии, оппозиционных российских вебсайтов спровоцировали множество вопросов, причем многие из них действительно до сих пор остаются без ответа.

Однако, будучи не российским официальным лицом, а независимым исследователем и экспертом, я могу сказать, что все подобные мнения и слухи не имеют ничего общего с реальностью. На самом деле в России на данный момент существует свободная система и достаточно либеральная модель регулирования интернета, особенно по сравнению с Казахстаном, Китаем, Ираном или Туркменией. В частности, отсутствуют какие-либо серьезные ограничения на поток информации в Сети, нет цензуры в отношении интернет-транзакций, что, конечно, отличается от ситуации с телевидением или радиовещанием. В России интернет действительно остается зоной свободных коммуникаций. В этом плане Россия имеет очень хорошую *кредитную историю*, что весьма актуально, когда речь заходит об информационной безопасности и управлении интернетом. Более того, политические заявления российского руководства до последнего времени демонстрировали готовность правительства не вводить никаких ограничений на свободу в интернете. Это хорошо, поскольку определенные идеи насчет введения подобных ограничений все же обсуждались и продолжают обсуждаться на высоком политическом уровне.

Однако российское правительство внесло определенные предложения, которые не находят единогласной поддержки на международном уровне. В частности, речь идет о концепции Конвенции об обеспечении международной информационной безопасности и предлагаемых *Правилах поведения в области обеспечения МИБ,* проект которых был направлен генсеку ООН четырьмя государствами — членами Шанхайской организации сотрудничества (ШОС) при ведущей роли России. Иногда эти инициативы воспринимают как российскую реакцию на американские концепции и стратегические документы, опубликованные чуть раньше, в прошлом 2011 г. Но если изучить и проанализировать *концепцию Конвенции об обеспечении МИБ*, становится ясно, что в этих предложениях нет ничего особо опасного, странного или неприемлемого для международного сообщества. Концепция Конвенции содержит ряд весьма востребованный сегодня определений: что такое кибервойна, или, точнее говоря, что такое информационная война, что такое информационное оружие, информационные системы, пусть эти определения в текущей редакции и не бесспорны.

В России избегают использования приставки *кибер-*, вместо нее предпочитают использовать прилагательное *информационный*. Концепция Конвенции перечисляет многие угрозы миру и международной безопасности, в том числе деструктивные действия в информационном пространстве, диверсионные действия, психологические войны, информационную экспансию. Возможно, иногда это действительно напоминает риторику холодной войны, когда у нас часто велась речь об *идеологической войне* американцев против Советского Союза. Сейчас существуют некоторые отличия, но эта угроза входит в список основных угроз, выделяемых авторами документа. В этой связи нельзя забывать о существовании принципов международного информационного права. Основным принципом является суверенитет государства над национальной инфраструктурой. На практике этот принцип означает, что все, что технически и физически расположено в пределах российских границ, должно регулироваться российскими законами.

Именно так Россия и некоторые другие страны хотят воплощать в жизнь принцип своего суверенитета над собственным киберпространством — или информационным пространством. В инициативах России и стран ШОС также прописаны меры по предотвращению военных конфликтов, информационных войн, меры по борьбе с терроризмом в киберпространстве, меры по борьбе с киберпреступностью, в том числе уголовные и другие правовые меры.

К сожалению, эти предложения были встречены многими государствами и экспертными сообществами весьма прохладно. Каковы причины столь негативного отношения? Причиной *номер один* является то, что при подготовке и инициировании этих предложений не применялся принцип участия всех заинтересованных сторон. Не применялся он и при обсуждении этих предложений на международном уровне. Российское интернет-сообщество не было приглашено к участию в разработке этих предложений, и поэтому в них присутствуют определенные ошибки, пробелы, а местами, может быть, и недостаточно хорошо проработанные, с юридической точки зрения, формулировки. Естественно, это не позволяет представителям российского экспертного сообщества безоговорочно поддержать подобные идеи. Но я бы хотел еще раз подчеркнуть, что фундаментальных изъянов в российских предложениях нет.

Что же касается суверенитета России над технической инфраструктурой в российском информационном пространстве, то здесь требуются дальнейшие теоретические исследования, чтобы понять, должен ли такой суверенитет быть абсолютным. К примеру, Олимпийские игры — это полностью неправительственное мероприятие, которое вносит многомиллиардный финансовый вклад в экономику многих стран, которые их принимают, организуют и участвуют в них. Но если Олимпийские игры проводятся в такой стране, как Россия, то есть игры в Сочи в 2014 г., то для их обеспечения будет использоваться инфраструктура и техническое оборудование, находящиеся в России. Несмотря на это, правила игр не могут определяться российским ФСБ или даже российским правительством — они определяются Международным олимпийским комитетом (МОК). При этом все страны, в том числе Россия, признают, что некоторые виды деятельности регулируются правилами, которые не могут определяться национальным законодательством, иначе они становятся невозможными.

Естественно, такие предложения требуют обсуждения, и необходимо еще более детально обсудить российские предложения в области МИБ. Возможно, нам следует обсуждать их в свете американских концепций и предложений, изложенных в национальной стратегии по действиям в киберпространстве американского Белого дома от 2011 г. Но есть еще один важный вопрос: следует ли нынешние (либо возможные будущие) российские предложения рассматривать как альтернативу или замену Будапештской конвенции *О киберпреступности*, которую Россия не подписала и не ратифицировала? Как уживутся эти документы? Будут ли они конкурировать или взаимно дополнять друг друга? Это открытый вопрос, требующий не менее пристального внимания.

ОРЛОВ: В докладе М. В. Якушева была затронута тема баланса между правительственными и неправительственными дискуссиями в России касательно роли интернета, будущего *Рунета* и информационной безопасности. Есть некоторые замечательные российские авторы, которые предполагают, что через 20–30 лет в России уже не останется *сети интер-нет*, а вместо нее будет лишь *сеть интерда*, которая будет автоматически одобрять все правительственные решения. Один из этих авторов — Владимир Сорокин, который отлично пишет на эту тему. Но судя по тому, что мы сейчас видим и слышим, такие пессимистические прогнозы, конечно, кажутся неоправданными. Я бы даже сказал, что российские власти и российские госструктуры сейчас довольно внимательно прислушиваются

к взглядам сообщества российских неправительственных организаций, особенно тех организаций, которые действительно разбираются в своих вопросах.

М. В. Якушев скромно не упомянул о своем участии в четырехчасовой встрече представителей российского интернет-сообщества с Д. А. Медведевым в 2011 г., когда тот занимал должность президента России. Мне было очень интересно читать протокол той встречи: президент часто использовал английские слова, потому что трудно было подобрать подходящие русские. В ходе встречи и общения президента с ее участниками также высветилось немало противоречий, которые я бы назвал *позитивными противоречиями*.

ВИКТОР ВАСИЛЬЕВ (ПОСТОЯННОЕ ПРЕДСТАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ООН И ДРУГИХ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЯХ В ЖЕНЕВЕ): Не могу согласиться с некоторыми высказанными сегодня взглядами. Один из них — это представление о том, что Россия якобы имеет *плохую историю* в сфере информационной безопасности. Я бы сказал, что у Российской Федерации, напротив, вполне позитивная история в этой области. Именно наша страна первой из всех государств подняла вопрос информационной безопасности на международной арене — мы сделали это в 1998 г. на площадке ООН. С тех пор мы выступили соавторами всех резолюций Генеральной Ассамблеи ООН по вопросам информационной безопасности. Конечно, у нас проходят плодотворные дискуссии, и российские участники уже неоднократно высказывали свои взгляды на эти вопросы. Мы понимаем, что точки зрения по разным аспектам могут отличаться, поскольку обсуждается очень широкая и сложная проблематика. Конечно, есть вопрос свободы слова, свободы информации и другие связанные вопросы.

Российская позиция как раз и представляет попытку инициировать обсуждение комплекса проблем, составляющих *триаду* информационной безопасности. Несмотря на то что многие западные страны могут не разделять российские взгляды, отраженные в наших документах, то есть в концепции Конвенции об обеспечении МИБ и в проекте Правил поведения в области обеспечения МИБ. Поэтому сейчас Россия и ее партнеры закладывают фундамент для такого обсуждения, представляют российскую позицию по некоторым вопросам, и мы выступаем соучастниками этой дискуссии. Мы также выделяем финансирование Институту ООН по исследованию проблем разоружения, который в этом году проводит ряд мероприятий в этой сфере, а также оказывает экспертную поддержку Группе правительственных экспертов (ГПЭ ООН) по МИБ. Группа представит свои взгляды на сессии Генеральной Ассамблеи ООН по вопросам информационной безопасности, запланированной на 2013 г.

Я считаю, что основной задачей для нас и наших партнеров является поиск точек соприкосновения по данным проблемам. Конечно, по некоторым вопросам у нас будут разногласия ввиду разных правовых подходов, различной доктринальной логики и т.д. Но есть и вопросы, по которым мы единодушны: это вопросы терроризма, преступной деятельности в интернете, проблемы мошенничества с кредитными картами, детская порнография и т. п. Нужно определить те сферы, где мы можем сотрудничать на международном уровне, где мы можем ввести нормы, которые помогут предотвратить подобные нарушения и которые будут способствовать успеху дискуссии на международном уровне по широкому кругу вопросов, в том числе по вопросу *красной кнопки* и т.д. Для этого нам нужна площадка для обсуждения, нам необходим форум. Нужно также решить, какие из существующих площадок лучше всего подходят для этих целей, имея в виду прежде всего ООН, МСЭ, Всемирную организацию интеллектуальной собственности (ВОИС) и ЮНИДИР, в рамках которых ведется обсуждение различных элементов информационной безопасности. Так что давайте над этим работать, давайте обдумывать эти вопросы и решать, в каких областях мы можем сотрудничать на практическом уровне.

БЕЙСЛИ-УОКЕР: Как только что отметил г-н Васильев, в российской концепции Конвенции об обеспечении информационной безопасности нет фундаментальных изъянов. Я не хотел бы сейчас давать оценки российскому предложению, но у меня нет сомнений, что между позициями американского и российского правительства существуют огромные различия на самом фундаментальном концептуальном уровне. Если попытаться более детально вникнуть в этот сюжет, становится очевидно, что мы имеем дело с двумя фундаментально разными по своей природе ответами на вопрос о том, является ли информация сама по себе оружием или нет. Возвращаясь к точке зрения В. Л. Васильева, я бы предположил, что в сегодняшних условиях международному сообществу будет крайне трудно достичь согласия, если не снять с повестки дня такие вещи, как российский проект глобального и юридически обязывающего документа ООН в области регулирования киберпространства. Есть много конкретных областей, по которым действительно можно достичь согласие, и мы не должны позволить определенным глобальным политическим вопросам затмить целый ряд потенциальных практических решений в рамках *мягкого* права, мер по укреплению доверия или правил поведения.

РИД: Продолжая мысль г-на Бейсли-Уокера, с точки зрения США я бы упомянул следующие моменты. Конечно же, перед нами стоит ряд вопросов в области безопасности, ряд вопросов в области киберпространства (как уже было отмечено, мы используем разные термины: с одной стороны, информационные и телекоммуникационные технологии, с другой — приставка *кибер*-). Но я полностью согласен с мыслью о том, что различия в терминологии или даже в концептуальном понимании не должны препятствовать нашему сотрудничеству. Мы рады тому, что эта беседа состоялась, мы также рады, что Россия еще в 1998 г. поставила на повестку дня ООН вопрос о глобальном регулировании информационной безопасности в рамках Объединенных Наций. Мы с большой готовностью подключились к этому процессу. Эти вопросы приобретают все большую важность в российско-американских двусторонних отношениях. Они получили развитие в виде обсуждения мер по укреплению доверия в наших двусторонних отношениях. Мне кажется, направленность американского взаимодействия с Москвой в данной области должна и впредь состоять в том, чтобы не позволить терминологическим противоречиям и дискуссиям, которые могут тянуться десятилетиями, помешать нам понять друг друга на практическом уровне, поддерживать контакты и сотрудничать во многих конкретных областях, где у нас есть общие цели. Поэтому мне кажется, что нужно идти путем мер по укреплению доверия, и здесь мы рассчитываем на межправительственную поддержку. Именно здесь мне видится весьма многообещающий потенциал для сотрудничества.

КИБЕРУГРОЗЫ И КИБЕРВЫЗОВЫ

ЯКУШЕВ: Международные форумы по вопросам управления интернетом проводятся ежегодно. Существует сеть региональных, местных и национальных форумов по управлению интернетом, которые проводятся в разных странах, в том числе и в России. Давайте сконцентрируемся на таком конкретном аспекте глобального управления интернетом, как *интернет-безопасность*. Существуют три или четыре уровня, которые требуют разных методов регулирования и которые имеют различные последствия в плане глобальной информационной безопасности.

- Проблема предотвращения *кибервойн* относится к уровню международных и межправительственных отношений, уровень международного права.
- *Кибертерроризм* и предотвращение атак, имеющих в своей основе политическую мотивацию и направленных против правительств, государственных органов и общества в целом.

- *Киберпреступность* — преступления, совершаемые обычными гражданами и пользователями интернета, в том числе такие незаконные действия, как мошенничество, кража личных данных и т.д. К сожалению, такие преступления в настоящее время широко распространены, более того, глобальный и национальные рынки киберпреступности активно развиваются и растут.

За последние пять лет в глобальной сети были отмечены определенные тенденции, связанные с развитием этой *триады угроз*. Мы видим необходимость в принятии мер, направленных против незаконного использования интернета и на недопущение его использования с целью подрыва международной безопасности. В основном об этом принято говорить в связи с такими инцидентами, как кибератаки в Эстонии, которые произошли пять лет назад (в 2007 г.) и были направлены против важных ресурсов и объектов инфраструктуры, которым в течение длительного времени был нанесен существенный ущерб. Тогда в самой Эстонии и на международной арене присутствовало понимание того, что источник атак находится за пределами страны и что они представляют определенную форму внешнего вмешательства. Эстонцы подозревали, что все эти атаки были организованы российским правительством, которое, естественно, опровергало обвинения, не имеющие под собой твердых доказательств.

БЕЙСЛИ-УОКЕР: Я согласен с классификацией, которая разделяет угрозы безопасности киберпространства на кибервойны, кибертерроризм и киберпреступность. Но мне кажется, что в процессе нашего сегодняшнего обсуждения также высвечивается смешение этих категорий. Очень легко говорить о четких классификациях, но как только мы начинаем обсуждать их предметно, границы между ними начинают размываться. Конечно, это представляет собой проблему для международного сообщества — проблему проведения четких терминологических, концептуальных и, впоследствии, нормативных границ. Как это сказывается на попытках эффективного регулирования и эффективного дипломатического взаимодействия в сфере безопасности киберпространства? Как провести черту между организуемой и направляемой государством кибератакой и кибертерроризмом, то есть в тех случаях, когда неизбежно приходится принимать во внимание правовые режимы? Где проходит эта черта? На все эти вопросы до сих пор нет четких ответов.

ВЕБЕР: Мне кажется, нам нужно обсуждать общие темы, которые представляют интерес для многих стран, чтобы получить некий общий ответ. Сложность, конечно, состоит в том, что все говорят о необходимости борьбы с кибертерроризмом. Невозможно найти человека, который скажет, «да, кибертерроризм — это полезная вещь». Проблемы начинаются, как только задается вопрос, а что такое кибертерроризм и кто такие кибертеррористы? В разных странах определение терроризма очень сильно отличается, не говоря уже об отсутствии согласованного определения кибертерроризма, то есть концептуальные и терминологические трудности возникают в самом начале обсуждения.

ОРЛОВ: Позвольте мне привлечь внимание к Олимпийским играм 2014 г. в Сочи в контексте информационной безопасности. Этот вопрос находится в первых строках повестки дня новоизбранного президента Путина; он также очень интересует некоторые швейцарские компании, которые плотно участвуют в подготовке к играм. Несмотря на нерешенный вопрос о том, имеем ли мы дело с неправительственной, межправительственной или другой деятельностью, факт остается фактом — война вокруг Олимпийских игр уже началась. Официальный российский вебсайт игр уже подвергся атаке в 2011 г., его работа была парализована на несколько дней. Этот эпизод стал явным сигналом того, что с приближением игр кибервойна вокруг них станет еще более ожесточенной.

Я бы хотел высказать некоторые соображения нашим швейцарским коллегам, которые так успешно выступают в роли посредников между Россией и Грузией.

В киберпространстве выступать в роли посредника очень нелегко. Как предотвратить DDoS-атаки? Кто является владельцем защитных систем — волшебных стен, которые выступят преградой на пути таких атак? Я выяснил, что сегодня в этой роли в качестве действительно серьезного игрока выступает всего лишь одна компания — американская компания, которая тесно связана с Министерством обороны США. Только у нее на самом деле есть эффективное решение против массированных DDoS-атак. Однако я надеюсь, что в России тоже будет достигнут прогресс в вопросах предотвращения таких видов кибератак.

Также заслуживает внимания корреляция между кибербезопасностью и другими видами угроз безопасности. Я имею в виду ядерную безопасность и атаки, направленные против ядерной инфраструктуры Ирана, которые оказались очень результативными. Эти атаки напугали иранцев, а израильтяне гордятся результатами атаки с использованием вируса *Stuxnet*. После этого по всему миру эхом прокатилась серия проблем, начиная от иранской ядерной инфраструктуры и заканчивая российскими объектами, по крайней мере в плане риска пролиферации таких атак. Кроме того, ракетные объекты Ирана тоже столкнулись со значительной угрозой — не физически, а через киберпространство. Это лишь один пример, близкий к тематике моих исследований. Но для меня он стал демонстрацией серьезности такого сочетания кибервойн и ядерной безопасности.

ВЕБЕР: В борьбе с кибератаками вопрос состоит в том, можно ли получить доступ к лицу, которое отвечает за конкретный IP-адрес. По крайней мере, согласно швейцарскому законодательству, это очень непростая процедура, она становится возможна только в случае проведения уголовного расследования. Существуют решения Верховного суда и Апелляционного суда кантона Берн, согласно которым частные организации, собирающие данные об IP-адресах, фактически не имеют права раскрывать эти адреса по каким бы то ни было причинам другим частным организациям, поскольку это будет нарушением законодательства о защите данных. Данное ограничение может быть снято, если ведется уголовное расследование. Прокурор имеет право попытаться установить личность, скрывающуюся за IP-адресом. Но, откровенно говоря, очень трудно понять, кому в таких случаях направлять свою жалобу. Кантону Женева? Федеральному прокурору? Какому-либо прокурору? Даже если мы получим ответ на вопрос о том, в какие органы следует адресовать тот или иной запрос, сразу возникает следующий вопрос: действительно ли в таких случаях применимо именно швейцарское законодательство? Трудно сказать. Возможно, применять следует законы не Швейцарии, а той страны, гражданином которой является конкретное лицо?

Таких вопросов очень много, и найти на них ответы нелегко. В области международного уголовного законодательства у нас также нет юридически обязывающих международных договоров, за исключением Конвенции Совета Европы *О киберпреступности*, которая действует на территории не только Центральной Европы, но и Восточной Европы, Средней Азии и даже в некоторых странах за пределами нашего континента. Однако, повторюсь, пока что у нас в этой области имеется больше проблем, чем решений.

НАДЕЖДА СИКОРСКАЯ (**NASHA GAZETA.CH**): Я — редактор русскоязычной швейцарской газеты, и у меня есть вопрос к участникам нашей дискуссии. Сайт *Нашей Газеты* в феврале 2012 г. подвергся нападению — DDoS-атаке с использованием ботнета — и едва не был полностью уничтожен, причем по непонятным нам причинам. С точки зрения содержания сайта, единственная возможная причина, которая приходит мне в голову, — это опубликованная статья на тему Олимпийских игр в Сочи, которая носила довольно критический характер. Кроме того, нападение произошло за несколько недель до президентских выборов в России, хотя по вопросу выборов мы не занимали какой-либо конкретной позиции. Тем не менее на нас напали, и на восстановление работы ресурса ушло довольно мно-

го времени, причем работа сайта восстановилась с большими трудностями. Наше расследование показало, что в качестве промежуточного звена при атаке были задействованы серверы, находящиеся на территории России и Китая. В то же время понятно, что такая информация не указывает на определение изначального источника атаки, поскольку можно использовать серверы-зеркала и другие технологии. Сайт нашей организации является русскоязычным, зарегистрирован в Швейцарии и размещен в домене *.ch*. Есть ли какая-то инстанция, куда мы можем направить жалобу? Кто занимается расследованием таких случаев и что мы можем сделать как пользователи и как жертвы нападения?

ЯКУШЕВ: Что касается незаконного использования интернет-технологий и технологий мобильной связи, то мы живем в мире, который с каждым днем становится все сложнее. Если вспомнить историю, поначалу даже практическое применение электричества или импорт картошки и помидоров из Америки в Европу создавали серьезные проблемы. Люди ели несъедобные части привозимых растений, например, ядовитые листья и цветки. Электричество также представляло опасность при неправильном обращении, не говоря уже об атомной энергии и более сложных технологиях. Аналогичным образом, у интернета есть как преимущества, так и недостатки, и нам нужно понять как сделать нынешний мир с его новыми технологиями безопаснее. К примеру, когда в 2011 г. в Лондоне прошли уличные беспорядки, резкой критике подверглось заявление британских властей о том, что они могут ввести определенные ограничения на доступ в интернет с коммуникаторов *Blackberry*. Всем было очевидно, что проблема заключалась не в интернете или интернет-технологиях, а в социальных проблемах в Великобритании. У нас нет *красной кнопки*, и мы не можем, к примеру, просто взять и навсегда отключить технологии *Blackberry* или интернет-соединение в масштабах страны.

Что же мы можем сделать? В первую очередь внедрить более совершенную систему идентификации граждан, которые используют определенные технологии коммуникации, мобильные телефоны и IP-адреса, доменные имена, и вести работу в этой области совместно с Обществом Интернета (ISOC). Я думаю, что российские и иностранные неправительственные организации, российское правительство и российские правоохранительные органы должны работать сообща, чтобы добиться осязаемых и положительных результатов, ничего при этом не запрещая неизбирательно и делая использование новых технологий безопаснее.

ПРОБЛЕМА *КРАСНОЙ КНОПКИ* — ОТКЛЮЧЕНИЕ ИНТЕРНЕТА

ЯКУШЕВ: В ходе нашей дискуссии мы также не можем не принимать во внимание пример *Арабской весны*, когда социальные сети сыграли определенную роль в ее событиях, помогли вывести людей на улицы и организовать акции, которые в итоге закончились сменой политического режима в данных странах и социально-политическими переменами. Пример Египта весной 2011 г. вновь продемонстрировал так называемую проблему *красной кнопки,* то есть масштабного целенаправленного отключения интернета на территории суверенного государства.

Египетский прецедент ставит нас перед массой вопросов, которых мы сегодня еще не касались. Можно ли отключить интернет на глобальном уровне или, возможно, существуют варианты его пошагового отключения на национальном уровне? Могут ли в киберпространстве применяться принципы, определяющие фундаментальные права человека? Какие виды деятельности нельзя допускать в Сети? Как выработать необходимые правила, которые учитывают основные права и свободы человека — к примеру, свободу слова, свободу распространения информации, свободу доступа к информации и доступа к интернету? Все эти вопросы однозначно должны быть вынесены на обсуждение.

ВАСИЛЬЕВ: Вопрос, который М. В. Якушев назвал проблемой *красной кнопки*, состоит прежде всего в том, кто контролирует *красную кнопку* и при каких обстоятельствах она может быть нажата. Каков политический и правовой порог для использования *красной кнопки* с целью отключения интернета? События *Арабской весны* невольно заставляют задуматься о любопытной тенденции. Если в содержании сетевых протестов присутствуют политические лозунги, такие как призывы к независимости и свободе, которые апеллируют к правам человека и так далее, нажимать *красную кнопку* нельзя. Получается, использовать ее можно только против хулиганов, координирующих свои действия в Сети, что обсуждалось властями Великобритании во время лондонских беспорядков 2011 г.? Это еще одна тема для широкой дискуссии.

Далее, профессор Вебер затронул вопрос выхода в интернет через мобильные телефоны. Дело в том, что во многих странах нет объективной необходимости контролировать связь между мобильными телефонами и провайдерами вебсайтов. Но давайте возьмем, к примеру, Россию, где теракты на Северном Кавказе происходят с достаточно высокой интенсивностью. Наглядный пример: когда произошли взрывы в московском метро в 2011 г., нашим службам безопасности пришлось отключить доступ в интернет с мобильных устройств, чтобы предотвратить дальнейшие взрывы. Такое решение было принято с учетом того, что некоторые из использованных взрывных устройств управлялись и приводились в действие при помощи мобильных телефонов. Очевидно, что в таких случаях ограничение мобильной коммуникации необходимо и действия спецслужб не следует рассматривать в качестве негативного примера использования *красной кнопки*.

ВЕБЕР: У меня есть короткий комментарий к очень интересной мысли, которую высказал г-н заместитель посла. Насколько я помню, я ни разу не упоминал прямые сравнения между разными странами, потому что хорошо понимаю: экспертам не следует *показывать пальцем* на те или иные страны. Тем не менее, поскольку я занимаюсь преподавательской деятельностью в Восточной Азии, хотелось бы привлечь ваше внимание к ситуации с *красной кнопкой* в этом регионе. Считается, что среди восточноазиатских государств нажать *красную кнопку* чаще всего пытается Китай. Однако, с другой стороны, *красную кнопку* также довольно часто нажимает Сингапур, который, как мы знаем, коммунистической страной не является. Так что нам нужно быть очень осторожными, когда речь заходит о сравнительных оценках государств в части свободы интернета. Технологически легче отключить мобильные телефоны, чем традиционные компьютерные сети — по крайней мере, если компании заинтересованы в сотрудничестве с правительством. Именно так и было в случае с Египтом в 2011 г., где интернет отключили, поскольку в определенный момент об этом настойчиво попросило правительство.

ЯКУШЕВ: Что касается самого понятия *красной кнопки*, то это, конечно, фикция. В прошлом сентябре я был в штаб-квартире ICANN и постарался обойти там все кабинеты — никакой *красной кнопки* я не нашел. Кое-кто утверждает, что *кнопка* находится в вашингтонском офисе, так что, может быть, я просто проверял не в том месте, ведь я был в Калифорнии. Что же касается *красной кнопки* в России, то я искренне горжусь тем, что живу в стране, где подобные технологии и методы никогда не использовались — и с этой точки зрения в нашей стране действительно отсутствует цензура в интернете. Мы должны этим гордиться.

КУММЕР: У нас состоялась интересная дискуссия по поводу *красной кнопки*, и я думаю, что г-н Вебер и г-н Васильев уже дали ответ на этот вопрос. Иногда эту кнопку также называют *рубильником смерти [killer switch]*. Технические эксперты использовали этот термин, когда обсуждался вопрос о том, как удалось так быстро отключить интернет в Египте во время событий *Арабской весны*. По существу, ответ заключается в том, что архитектура глобальной сети в республике была очень несовершенна: чрезмерно централизована. Если архитектура интернета

спроектирована должным образом, то это очень распределенная и очень устойчивая система. Ведь в свое время именно такая задача была поставлена перед теми, кто стоял у истоков интернета: создать сеть, которая сможет выдержать даже массированный ядерный удар. Во время природных бедствий, таких как цунами в Японии в 2011 г. или землетрясение на Гаити в 2010 г., интернет оказался едва ли не единственным работающим средством связи. Вся остальная инфраструктура, за исключением спутниковой связи, вышла из строя, а интернет продолжал функционировать, и люди могли связаться друг с другом через Сеть. Поэтому если архитектура интернета спроектирована и сбалансирована должным образом, то никакого *рубильника смерти* в Сети не существует.

Что же касается международного сотрудничества, то оно просто незаменимо. Мы должны сотрудничать и мы должны вести обсуждения. Рассматриваемая нами проблема имеет много общего с терроризмом: общепринятого определения того, что такое терроризм, на международном уровне до сих пор не существует. То же самое можно сказать о детской порнографии и массе других проблем, связанных с безопасностью киберпространства. Общепринятых и универсальных определений этих проблем у нас пока нет. Ключевой международной площадкой для обсуждения проблем и определений является Форум по управлению интернетом, который работает под эгидой ООН, созывается от имени генерального секретаря ООН и в котором участвует множество стейкхолдеров. При поиске решений необходимо прислушиваться ко мнению всех стейкхолдеров. Государство и правительство находится на острие решения проблем безопасности, однако очень важно, чтобы власти прислушивались к тому, что говорит гражданское общество, у которого обычно существуют серьезные озабоченности в сфере прав человека. Не менее важно также обсуждать с техническим экспертным сообществом вопрос о том, насколько осуществимы предлагаемые технологические меры решения. И, конечно же, все стейкхолдеры должны работать и действовать сообща.

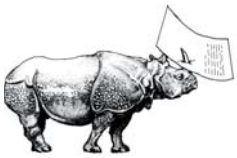
ОРЛОВ: Большое спасибо! Я думаю, что нам уже удалось многого добиться во время сегодняшней встречи, особенно благодаря нашим докладчикам, основному докладчику и комментатору. Я очень ценю работу и усилия, предпринятые г-ном Якушевым и профессором Вебером, и я уверен, что нам еще есть много что сказать, так что наш разговор не ограничится сегодняшней встречей. Мы бы хотели объединить усилия и в ближайшие месяцы принять участие в дальнейшей широкой международной дискуссии по поводу принципиальных вопросов кибербезопасности и управления интернетом.

В 2013 г., на следующем ежегодном заседании с участием членов *Centre russe d'etudes politiques* и сообщества Международного клуба *Триалог* мы планируем обсудить довольно близкие темы, такие как новые угрозы безопасности, в том числе финансовые преступления и вопросы связи между отмыванием денег, терроризмом и финансированием программ по разработке оружия массового уничтожения. Однако тема, которую мы обсуждали сегодня, вне всяких сомнений, остается одним из основных направлений исследований, проводимых ПИР-Центром, в рамках которого активно развивается проект «Международная информационная безопасность и глобальное управление интернетом». Пока что проект базируется преимущественно в Москве, однако широкое и интенсивное сотрудничество с иностранными экспертами, аналитическими центрами и международными организациями станет важным шагом в дальнейшем развитии нашего проекта. Ряд проблем, которые мы сегодня затронули, требуют быстрого и хорошо продуманного вклада неправительственного сообщества, в том числе ПИР-Центра, в обеспечение процесса принятия политических решений в России соответствующей аналитической базой.

Национальная политика в области защиты критической инфраструктуры пока не приобрела в России системного характера. Еще только предстоит решить, какой

подход должен использоваться в данной сфере. Кроме того, по мере быстрого развития российского рынка киберпреступности нарастает обеспокоенность в связи со все более изощренными, многочисленными и масштабными преступными действиями как в национальных российских сетях, так и за их пределами. Здесь, как уже было отмечено докладчиками и комментаторами, Россия должна предложить собственный подход к развитию эффективного международного сотрудничества по борьбе с киберпреступностью, поскольку Будапештская конвенция, похоже, не рассматривается в качестве оптимальной основы для российского участия в подобных механизмах. Наконец, благодаря всем участникам сегодняшней встречи, мы получили весьма подробную и разноплановую картину стратегических дискуссий в области межправительственного регулирования вопросов информационной безопасности, включая предложения в этой сфере, внесенные Россией и государствами-членами ШОС.

Еще более важен тот факт, что мы, как это ни удивительно, пришли к очень четкому общему пониманию того, что нужно делать, для того чтобы стимулировать сотрудничество между Россией и ее западными партнерами, несмотря на то что пока между нами сохраняются определенные противоречия. Прозрачность и меры по укреплению доверия, пошаговый подход, много- и двусторонние компромиссы, обмен информацией и постоянные интенсивные дискуссии с широким участием НПО и экспертного сообщества не являются панацеей, но они представляют собой проверенный и безотказный рецепт. Сегодня мы здесь собрались, чтобы заставить этот рецепт работать. Я убежден, что в ходе сегодняшнего заседания мы уже внесли свой вклад в эту грандиозную задачу — конструктивный вклад, направленный на проработку этого крайне важного глобального вопроса. Теперь наша цель в том, чтобы продолжить этот позитивный процесс. Я надеюсь, что эта встреча станет лишь первым шагом в длительном системном процессе, который объединит усилия российских, западных и многих других экспертов и ответственных лиц, направленные на укрепление безопасности киберпространства и обеспечение беспрепятственного использования информационных технологий по всему миру.



Хамадун Туре

КИБЕРУСТОЙЧИВОСТЬ: СУТЬ МИРА В КИБЕРПРОСТРАНСТВЕ[1]

Мне хотелось бы сказать несколько слов о ***киберустойчивости***, в которой, по моему мнению, заключается суть мира в киберпространстве. Всемирная федерация ученых и ее Постоянная группа по мониторингу информационной безопасности внесли весомый вклад в поддержание ядерного мира в период холодной войны, когда ядерная гонка вооружений достигла своего пика. В современных условиях, когда киберпространство превратилось в столь сложный феномен, а информационные и коммуникационные технологии (ИКТ) играют ключевую роль в социальном и экономическом развитии, я рад, что Всемирная федерация ученых и Постоянная группа по мониторингу информационной безопасности снова помогают миру тем, что обеспечивают участие науки и ученых в борьбе со все возрастающими угрозами, которые подстерегают нас в киберпространстве.

Мы живем в мире, в котором количество абонентов мобильной связи перевалило за 6 млрд, а число пользователей интернета вскоре достигнет 2,5 млрд. Эта глобальная *гиперконнективность* дает нам возможность использовать силу технологий, особенно мобильных технологий, для того, чтобы сделать мир, в котором мы живем, еще лучше. Однако, к сожалению, эта новая инфраструктура, без которой уже невозможно себе представить современную жизнь, приносит и новые вызовы миру и стабильности.

Все мы видим растущее количество уязвимостей и угроз в киберпространстве, которые оказывают непосредственное воздействие и на реальный мир. К их числу относится, например, обнаруженный в 2010 г. вирус *Stuxnet*, создатели которого взяли под прицел иранский завод по обогащению урана (т.е. конкретный промышленный объект), вирус *Duqu*, найденный в 2011 г., который среди прочего имел своей целью сбор информации о промышленных системах, или вирус *Flame* в 2012 г., который предназначался для сбора данных в незаконных целях.

Мобильная связь сейчас является основным двигателем роста интернета: к концу прошлого года количество абонентов *3G* достигло почти полутора миллиардов. За один 2011 г. во всем мире было продано порядка 1,7 млрд многофункциональных телефонов и смартфонов. По мере роста продаж смартфонов мобильная связь предоставляет все новые возможности для совершения потенциально прибыльных киберпреступлений, а киберпреступники чрезвычайно быстро учатся пользоваться этими новыми возможностями.

В прошлом году впервые мобильные вирусы стали реальной угрозой как для компаний, так и для потребителей, и можно ожидать, что эта тенденция сохранится по мере того, как создатели вирусов будут изобретать все новые способы атаковать мобильные телефоны и планшетные компьютеры. Только за первые несколь-

ко месяцев 2012 г. на одной из наиболее распространенных мобильных платформ было обнаружено около 25 тыс. новых угроз. Еще одной интересной новой тенденцией стало изменение природы спама: в 2010 г. на долю спама приходилось 88,5% всех электронных почтовых сообщений, тогда как в прошлом году эта цифра сократилась до 75,1%. Похоже, что спамеры сейчас уделяют больше внимания социальным сетям, чем обычной электронной почте.

Распространение вредоносного кода, поражающего продукцию компании *Apple*, также растет, и эта тенденция сохранится и в 2012 г., по мере того как этот код становится частью более широкого хакерского инструментария. На самом деле в этом нет ничего удивительного, поскольку киберпреступления приносят все бо́льшие доходы: речь идет уже не о миллионах, а о миллиардах долларов ежегодно. Более того, киберпреступность может стать гораздо более опасным явлением, чем она была в прошлом, поскольку роль ИКТ в управлении критическими важными объектами инфраструктуры и их мониторинге неуклонно растет, и государства все больше полагаются на них.

В прошлом году кибератаки стали более целенаправленными и более политически и финансово мотивированными, а количество случаев утечки данных и атак на органы сертификации выросло до небывалого уровня. Правительственные и общественные организации наиболее часто подвергались атакам через электронную почту, при этом риски для компаний как малого, так и крупного бизнеса тоже росли. В этой связи я очень рад, что Международному союзу электросвязи (МСЭ) совместно с *Лабораторией Касперского* и в рамках сотрудничества МСЭ с Международным многосторонним партнерством против киберугроз (IMPACT), удалось обнаружить вирус *Flame* на начальной стадии и незамедлительно предупредить государства — члены МСЭ и соответствующие органы ООН. А 10 августа 2012 г., снова в партнерстве с *Лабораторией Касперского*, мы обнаружили еще одно кибероружие под названием *Gauss*, которое было специально разработано для отслеживания электронных банковских счетов и связанной с ними конфиденциальной финансовой информации.

При наличии компьютерных вирусов и кибероружия развитые информационно-коммуникационные сети все больше привлекают внимание тех, кто хочет использовать их в террористических или шпионских целях, создавая новую концепцию войны — кибервойну. Кибервойны начинаются в киберпространстве с использованием ИКТ, но они могут стремительно распространиться за пределы виртуального мира, нанося ущерб правительствам, компаниям и обычным людям. Нам необходимо серьезно задуматься над тем, какой глобальный негативный эффект это может иметь для международной безопасности, и забыть на время о своих политических и иного рода разногласиях.

Для обеспечения мира в киберпространстве нам необходима *киберустойчивость*, а для этого надо взглянуть на пять стратегических направлений Глобальной программы кибербезопасности (ГПК).

Кибербезопасность — это многогранная тема, имеющая несколько измерений. Безопасность на уровне отдельных пользователей подразумевает отсутствие киберугроз, таких как компьютерное мошенничество, незаконная обработка электронных данных, кража персональных данных, детская порнография и т.д. Вредоносная деятельность в киберпространстве несет высокую степень угрозы для национальной безопасности. Без обеспечения безопасности как для частных пользователей, так и для целых стран невозможно достичь международной безопасности. Для обеспечения кибербезопасности в глобальном масштабе необходимо сформировать международную культуру кибербезопасности.

МСЭ, специализированное учреждение ООН в области ИКТ, является глобальной и непредвзятой организацией. Мы по праву гордимся работой, которую мы проводим в рамках нашей ГПК.

ГПК состоит из пяти ключевых направлений, которые в совокупности представляют собой основные меры для достижения киберустойчивости и укрепления мира и стабильности в киберпространстве. Эти пять направлений включают:

- правовые меры, которые играют роль сдерживающего фактора для киберпреступников и одновременно обеспечивают адекватное реагирование на киберпреступления;
- технические и процедурные меры, которые используют сами технологии и технические средства для повышения устойчивости систем к кибератакам;
- организационные структуры, необходимые для укрепления сотрудничества и партнерства между всеми заинтересованными сторонами;
- создание потенциала, необходимого для повышения осведомленности и понимания технологий, которыми мы пользуемся;
- международное сотрудничество, о котором я скажу ниже.

На основании работы, проведенной в рамках ГПК, чтобы найти комплексное решение проблемы киберустойчивости, следует рассмотреть следующие вопросы:

- доступ в интернет;
- защита основных прав (включая право на частную жизнь и свободу выражения);
- роль государства;
- международное сотрудничество.

Доступ в интернет. Интернет стал совершенно необходимым инструментом развития, и обеспечение всеобщего доступа к интернету должно быть приоритетом для всех государств. Однако для сокращения *цифрового разрыва* требуется обеспечить не только доступ в интернет. Люди должны также иметь возможность использовать информационные и коммуникационные технологии в целях индивидуального и коллективного развития.

В своих усилиях по преодолению *цифрового разрыва* государства должны стремиться обеспечивать всеобщий доступ к информации и знаниям, высокое качество образования для всех граждан, уважение к культурным и языковым различиям и защиту основных прав. Более того, развитие информационного общества требует, чтобы у каждого человека был доступ к средствам коммуникации, местной инфраструктуре, недорогой связи и образованию в сфере использования ИКТ. Государства должны выработать действенный ответ на связанные с интернетом угрозы и уязвимости, уделяя особое внимание опасностям, которые подстерегают детей и подростков, и предоставляя гражданами цифрового мира эффективные механизмы для защиты себя и своих сообществ.

Защита основных прав (включая право на частную жизнь и свободу выражения). Когда государства предпринимают меры по обеспечению стабильности и безопасности киберпространства, борются с киберпреступностью и противостоят киберугрозам, они также должны уважать свободу в киберпространстве и основополагающие права пользователей. Это сложная и зачастую противоречивая тема, по которой идет оживленная дискуссия о том, как, с одной стороны, обеспечить безопасность, а с другой — защитить частную жизнь и другие права пользователей. И хотя некоторые стремятся противопоставить понятия безопасности и права на частную жизнь, важно подчеркнуть, что эти две цели отнюдь не являются взаимоисключающими. Безопасность необходима для обеспечения прав, таких как право на частную жизнь и свободу выражения, поэтому принципиально важно достичь обеих этих целей.

Когда речь заходит о киберустойчивости и кибербезопасности, нередко возникает опасность забыть о важности обеспечения таких основополагающих прав, как право на свободу мнений и выражения, право на информацию, право на частную жизнь и защиту персональных данных, свободу собраний и объединений и право на свободу от дискриминации.

Мне также представляется, что очень важно обеспечить максимально свободный всеобщий доступ к научным исследованиям в интернете, что послужит стимулом для инноваций, улучшит качество жизни и создаст столь нужные в XXI в. новые рабочие места, особенно для женщин и молодежи. Мы должны сделать все необходимое, для того чтобы сохранить наше культурное наследие в электронном виде для нынешнего и будущих поколений. Все мы знаем, какое значение имеют в реальном мире библиотеки, музеи и архивы. В виртуальном мире их значение еще больше, потому что там они доступны всем людям на земле.

Роль государства. Любое действие, подразумевающее участие государства, будь то в реальном или в виртуальном мире, должно совершаться с учетом принципов соблюдения прав человека, территориальной неприкосновенности и национального суверенитета. Кибератаки больше нельзя рассматривать как изолированные события. Государства и другие игроки должны быть осведомлены о потенциальном риске и опасностях, связанных с такого рода инцидентами.

Критические объекты инфраструктуры все чаще становятся мишенью кибератак. Их уничтожение или повреждение может серьезно подорвать безопасность государств и поставить под угрозу жизни людей. Если мы хотим сохранить наше общество, обеспечить функционирование системы общественного транспорта, коммунальных услуг и других систем, объекты критической инфраструктуры не должны подвергаться кибератакам. В отношении подобного рода инцидентов должны применяться международные правила ведения войн.

Чтобы создать более безопасные киберсреду и киберпространство, необходимы международное сотрудничество в этой области, последовательные усилия и настойчивость.

Международное сотрудничество. Для достижения киберустойчивости, а следовательно, обеспечения мира в киберпространстве, потребуется международное сотрудничество, при котором государства взаимодействуют друг с другом и принимают активное участие в совместных международных усилиях.

Киберпространство — явление глобальное, поэтому для укрепления киберустойчивости и обеспечения мира в киберпространстве потребуются глобальные усилия, в идеале в виде международного рамочного соглашения, которое учитывает потребности и желания всех его участников. Совместно, на международном уровне нам надо сотрудничать в области разработки и технического обеспечения технологий безопасности, которые защитят пользователей, в первую очередь детей и подростков, и помогут нам достичь глобальной киберустойчивости. Кроме того, государствам следует делиться друг с другом передовыми методами работы и опытом, а также распространять технологии, помогающие повысить уровень доверия в киберпространстве.

Нам также следует развивать международное сотрудничество в сфере электронных финансовых операций в целях предотвращения таких преступлений, как отмывание денег, которым в виртуальном мире помогают системы киберплатежей или, например, электронные казино. В одиночку государствам с этим не справиться. Они должны действовать в тесном взаимодействии с другими заинтересованными сторонами. В современном мироустройстве эффективное сотрудничество по таким комплексным направлениям, как киберустойчивость, должно осуществляться с участием гражданского общества, частного сектора, различных групп потребителей, региональных и международных организаций и других национальных и наднациональных игроков.

И, наконец, только посредством международного сотрудничества мы можем начать обсуждение таких важных вопросов, как ограничение распространения кибероружия и — в перспективе — полное разоружение в киберпространстве.

Вопросы кибербезопасности и киберпреступности актуальны для каждой страны, каждой компании и каждого отдельно взятого пользователя интернета. И когда мы говорим о том, что ООН должна активно заниматься поддержанием мира и безопасности, следует помнить, что в XXI в. безопасность и мир в киберпространстве являются неотъемлемой частью этого процесса.

Как руководитель МСЭ я прилагаю активные усилия, чтобы убедить страны, которые еще этого не сделали, присоединиться к 144 государствам, принимающим участие в совместной инициативе МСЭ и Международного многостороннего партнерства против киберугроз (ITU-IMPACT). Эта инициатива представляет собой первый поистине глобальный, многосторонний, государственно-частный альянс против киберугроз. Помимо этого я стараюсь привлечь в ITU-IMPACT частный сектор, а также межправительственные агентства и неправительственные организации. Мы должны сообща работать над установлением международных правил и стандартов, чтобы укрепить киберустойчивость посредством международной системы норм и принципов, регулирующих безопасность и мир в киберпространстве.

Поэтому я хотел бы призвать вас продолжать делать то, что у нас так отлично получается: работать вместе, прислушиваться ко всем участникам процесса и создавать лучшее будущее для всех людей на земле. Речь идет о создании мира киберустойчивости, где на смену киберугрозам и киберпреступлениям пришли бы безопасность и мир в киберпространстве.

В завершение позвольте задать несколько вопросов, которые должны определить ход дискуссии о киберустойчивости:

Как нам отставить в сторону свои идеологические и политические расхождения, чтобы вместе работать над установлением приемлемых для всех норм и правил поведения для частных лиц, правительств и компаний?

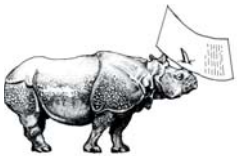
Как нам продолжить инновации в области разработки и использования ИКТ, одновременно обеспечивая право на частную жизнь и свободу выражения мнений?

Как нам внедрить надежные оборонительные и защитные системы раннего предупреждения о кибератаках, способные обеспечить защиту критических объектов инфраструктуры?

И, наконец, настроены ли мы на совместную работу для достижения нашей общей цели, обеспечения киберустойчивости?

Примечания

[1] Комментарий подготовлен на основе выступления Хамадуна И. Туре на 45-й сессии Международных семинаров по чрезвычайным ситуациям планетарного масштаба в Эриче, Сицилия, 20 августа 2012 г. с любезного разрешения Международного Союза Электросвязи. Перевод (с) ПИР-Центр, 2012 г.



Елена Зиновьева

ЦИФРОВАЯ ДИПЛОМАТИЯ, МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ И ВОЗМОЖНОСТИ ДЛЯ РОССИИ

Термин *цифровая дипломатия*, распространенный наряду с понятиями *интернет-дипломатия*, *дипломатия социальных сетей* и *Web 2.0 дипломатия*, впервые начал использовать применительно к внешней политике США. В частности, под ним подразумевалось широкое использование информационно-коммуникационных технологий (ИКТ), в том числе *новых медиа*, социальных сетей, блогов и тому подобных медиаплощадок в глобальной сети для содействия государственным органам для осуществления функций и коммуникаций по вопросам, связанным с внешнеполитической повесткой дня[1]. В настоящее время программы *цифровой дипломатии* реализуются не только США, но и рядом других государств. В частности, возможность перехода к *цифровой дипломатии* рассматривается также государствами НАТО[2].

ЭВОЛЮЦИЯ ТЕРМИНА И ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ

Правительство США определяет цифровую дипломатию как применение социальных сетей в дипломатической практике правительства США для обеспечения взаимодействия американских дипломатов с зарубежными пользователями интернета[3]. Цифровая дипломатия США — одно из направлений публичной дипломатии, ориентированной на вовлечение в дипломатическую практику широких слоев населения, а не на взаимодействие с политической и дипломатической элитой зарубежных государств. Как отмечает российский исследователь Н. А. Цветкова, методами *публичной дипломатии Web 2.0* являются «размещение радио- и телепередач в сети интернет, распространение в открытом доступе литературы о США в цифровом формате, мониторинг дискуссий в блог-пространстве, создание персонифицированных страничек членов правительства США в социальных сетях, а также рассылка информации через мобильные телефоны»[4].

Реализация программ *цифровой дипломатии* США проводится с опорой на крупные компании интернет-индустрии, среди которых лидирующие позиции занимает корпорация *Google*. Отправной точкой для активизации политики Государственного департамента в цифровой сфере стало осознание потенциала воздействия интернета на значительное число пользователей персональных компьютеров и обладателей мобильных телефонов в мире. Действительно, на сегодняшний день более 30 % населения планеты являются активными пользователями интернета, и цифра эта постоянно растет[5].

Ключевым для понимания сути *цифровой дипломатии* является тот факт, что она представляет собой *технологический* инструмент. В основе внешней политики и *цифровой дипломатии* Соединенных Штатов заложены идейные основания, которые эффективно воплощают бизнес-модель и информационная политика *Google*,

Facebook, Twitter и других компаний американской интернет-индустрии — и прежде всего ценность демократии и либеральных свобод. Философские основы *цифровой дипломатии* были изложены в трудах Энн-Мэри Слотер, которая с 2009 по 2011 г. занимала пост директора по политическому планированию в Государственном департаменте США. В частности, по мнению госпожи Слотер, государства, обладающие наиболее налаженными и разветвленными информационными каналами и коммуникациями, способны определять глобальную повестку дня[6].

Программы *цифровой дипломатии* в США получили развитие в 2002–2003 гг., когда администрация Джорджа Буша-младшего начала переносить традиционные радио- и телеканалы международного вещания в интернет. В 2006 г. госсекретарь Кондолиза Райс сформировала Группу цифрового взаимодействия, в состав которой вошли специалисты, занимающиеся мониторингом информации и дезинформации о США, которую транслировали пользователи в социальных сетях. Тогда же госсекретарь объявила о запуске первого официального блога Госдепа, открыла правительственный портал и несколько электронных журналов[7].

Хиллари Клинтон, получившая пост госсекретаря в администрации Барака Обамы в 2009 г., стала инициатором программы обновления внешней политики США, которая получила название «Государственное управление в XXI веке». Одним из направлений данной программы и стала цифровая дипломатия. Инициатива Госдепа предполагает дополнение традиционного инструментария внешней политики инновационными инструментами госуправления, которые будут направлены на то, чтобы полностью реализовать потенциал сетей, технологий, а также населения во взаимозависимом мире[8]. При Хиллари Клинтон цифровая дипломатия была выведена на новый политический уровень, перед ней были поставлены значимые для внешней политики США цели, такие как информационная дискредитация идеологии Аль-Каиды, Талибана и других различных антиамериканских движений, а также борьба против политических режимов в Иране, Китае и в ряде других стран посредством мобилизации протестного молодежного движения и нового движения диссидентов[9].

В настоящее время американские программы *цифровой дипломатии* реализуются в рамках различных ведомств, в том числе Госдепартамента, ЦРУ, Министерства обороны, а также Агентства международного развития США. Координацию публичной дипломатии в интернете по состоянию на сентябрь 2012 г. осуществляли заместитель госсекретаря по вопросам публичной дипломатии Тара Соненшайн, ответственная за продвижение в глобальной сети американских теле- и радиоканалов, ориентированных на зарубежную аудиторию, и старший советник по инновациям Алек Росс, занимающийся работой с социальными сетями.

В 2010–2011 гг. Белым домом были опубликованы несколько официальных документов, задающих направления *цифровой дипломатии*. В их числе был документ «Публичная дипломатия: укрепление взаимодействия Соединенных Штатов с миром»[10], где обозначались задачи, определяемые руководством США для цифровой дипломатии. В частности, в список таких задач вошли:

- дискредитация идеологических противников Соединенных Штатов;
- противодействие информационной деятельности Китая в интернете;
- ограничение медиаприсутствия России на пространстве бывшего Советского Союза;
- противодействие внешней культурной политике Ирана, осуществляемой через социальные сети[11].

В задачи *цифровой дипломатии* также входит поддержка молодежных движений. Одним из наиболее успешных стало организованное с помощью социальной сети *Facebook* движение, которое переросло в массовую волну протестов против Рево-

люционных вооруженных сил Колумбии — Армии народа в 2008 г.[12]. Чуть позже при американской инициативе был создан так называемый Альянс молодежных движений, который объединил молодых людей, желающих использовать новые технологии в политических целях. На сайте *Альянса* размещены инструкции по созданию блогов и запуску кампаний в социальных медиа[13].

Важную роль в осуществлении *цифровой дипломатии* США в странах Ближнего Востока играет Команда по цифровым внешним контактам (Digital Outreach Team), которая была создана в 2006 г. В задачи команды входит участие в дискуссиях по вопросам внешней политики США с пользователями популярных сайтов на арабском и персидском языках, а также урду. До середины 1990-х гг. публичная дипломатия США осуществлялась в основном при помощи Информационного агентства США, чьи методы работы предполагали лишь одностороннее взаимодействие. После начала войны в Ираке в 2003 г. администрацией Джорджа Буша-младшего был дан старт использованию радио и телевидения как инструментов публичной дипломатии. Однако население стран Ближнего Востока изначально относилось к предоставляемой информации с недоверием. В этих условиях стала очевидна необходимость диалога и *интерактивного* взаимодействия, что и стало целью создания Команды по цифровым внешним контактам. Согласно информации Бюро международных программ, миссия команды состоит в «разъяснении внешней политики США и борьбе с дезинформацией»[14].

Спустя несколько месяцев после речи Хиллари Клинтон о свободе интернета, в мае 2010 г. была опубликована Международная стратегия США по действиям в киберпространстве[15]. В соответствии с положениями документа, защита прав человека и прежде всего свободы слова в интернете является одним из приоритетов внешней политики США. В сентябре 2010 г. Госдепартамент разработал документ под названием «Стратегический план развития информационных технологий в 2011–2013 гг.: цифровая дипломатия»[16], в котором уточнялись и конкретизировались направления *цифровой дипломатии*, помещенные в контекст реализации внешнеполитических приоритетов Вашингтона. В частности, среди таких приоритетов значились обеспечение международной безопасности и формирование позитивного образа страны за рубежом.

Кроме того, реализация программ *цифровой дипломатии* предполагает следующие направления деятельности:

- финансирование проектов по созданию и распространению новых технологий, позволяющих обходить цензуру в сети;
- создание информационных сервисов, направленных на поддержку оппозиции в авторитарных странах;
- создание систем *теневого интернета* и независимых сетей мобильной связи, развертывание которых на территории третьих стран позволит борцам с авторитарными режимами обмениваться информацией в режиме онлайн, обходя запреты властей[17].

Параллельно в США был принят ряд документов, затрагивающих военно-политические аспекты развития интернета. В июне 2011 г. была частично опубликована Стратегия по действиям в киберпространстве Пентагона[18]. В этом документе киберпространство рассматривается как *пространство ведения боевых действий* наряду с наземным, морским и воздушным, а также космическим пространствами[19]. Стратегия Министерства обороны развивает подход ранее принятой администрацией Барака Обамы Стратегии национальной безопасности от 2010 г.[20], в которой киберпространство также рассматривается как потенциальное *поле боя*.

Как представляется, внешнеполитическая стратегия Белого дома в глобальной информационной сфере носит целостный характер и направлена на реализацию

американских национальных интересов. Таким образом, цели *цифровой дипломатии* следует рассматривать как взаимодополняющие по отношению к задачам военно-политического характера по обеспечению лидерства США в глобальной информационной сфере. Оценивая международную политику Соединенных Штатов в данной сфере, российский эксперт Е. А. Роговский приходит к выводу о том, что конечной целью является содействие достижению и удержания США глобального лидерства[21].

В 2011 г. программы *цифровой дипломатии* привлекли к себе существенное внимание, прежде всего, вследствие массовых волн протеста в странах Ближнего Востока и Северной Африки, получивших в прессе название *твиттер-революций*. Был опубликован ряд научных статей, оценивающих роль социальных сетей и новых медиа в так называемой *Арабской весне*. По мнению многих российских и зарубежных исследователей, движущей силой во всех протестных движениях была молодежь, которая стала совершенно новой, не оформленной идеологически политической силой. При этом была продемонстрирована самостоятельная роль интернета и СМИ. Однако в то же время, по мнению ряда экспертов, социальные сети, являясь нейтральными каналами коммуникации, не сыграли определяющей роли в событиях *Арабской весны.* Утверждается, что в данных событиях социальные сети выступили в роли катализатора массовых протестов, глубинные же причины происходящего были обусловлены конкретной социально-экономической, политической и религиозной ситуацией в этих странах[22].

Однако при этом важную роль в *направлении* и оформлении революций сыграла цифровая дипломатия США[23]. Официальная позиция Белого дома по поводу событий *Арабской весны* сформулирована в статье старшего советника Хиллари Клинтон по инновациям Алека Росса. Роль социальных сетей в революционных событиях на Ближнем Востоке оценивается как координирующая, однако не первостепенная[24]. Вместе с тем в той же статье отмечается трансформирующая роль ИКТ в политике и дипломатии. Утверждается, что цифровые технологии являются важным ретранслятором идей и в целом способствуют демократизации и *распылению власти*, как во внутренней, так и в международной политике, хотя и могут использоваться в своих целях диктаторскими и авторитарными режимами. Аналогичные идеи высказывает видный американский политолог Джозеф Най в своей последней книге *Будущее власти*[25].

Результаты исследования, проведенного в августе 2010 г. Институтом исследований мира США, показывают, что новые медиа оказывают влияние на общественное мнение, смягчают либо обостряют межгрупповые конфликты, способствуют коллективным действиям, провоцируют негативную обратную реакцию в государствах с авторитарными режимами, а также привлекают международное внимание к определенным странам. Вместе с тем авторы исследования полагают, что сделать однозначные выводы о влиянии социальных сетей на протесты и революции в странах Северной Африки и Ближнего Востока не представляется возможным. Традиционные СМИ до сих пор являются не менее, а зачастую даже более влиятельными по сравнению с социальными медиа[26]. Исследование *Гражданские инициативы: влияние Facebook и Twitter*, проведенное Дубайской школой управления, показывает, что социальные сети, пользователи которых все чаще ставят перед собой политические задачи, сыграли важную роль в мобилизации граждан и формировании общественного мнения. При этом любопытно, что количество пользователей социальной сети *Facebook* в первые месяцы 2011 г. выросло на 30 %[27]. Таким образом, исследователи приходят к схожим выводам о значимом, но не первостепенном влиянии социальных медиа на организацию массовых протестов и революций в странах Северной Африки и арабского Востока. Также нет единства в оценках роли программ *цифровой дипломатии* США как катализатора протестных настроений.

В исследовательском сообществе США отношение к *цифровой дипломатии* неоднозначно. Сотрудник Джорджтаунского университета Евгений Морозов обращает внимание на опасности, которые таит в себе широкое применение социальных сетей. Сервисы Web 2.0 предоставляют новые возможности не только дипломатам и прозападно ориентированным группам, но и радикальным организациям[28]. В свете недавних выборов в Египте, где по результатам парламентских выборов 2012 г. большинство мест в нижней палате получили представители политического крыла организации исламистского толка *Братья-мусульмане*, его выводы представляются не лишенными оснований. Более того, по мнению эксперта, глобальная сеть может не только служить эффективным инструментом демократизации, но и способствовать усилению авторитарных тенденций, ограничивающих свободу граждан.

Исследования эффективности программ *цифровой дипломатии* проводились Оксфордским университетом. Команда по цифровым внешним контактам Госдепартамента США инициировала ряд сетевых дискуссий, посвященных речи Барака Обамы в Каире в 2009 г. Контент-анализ сообщений пользователей показал, что их реакция на дискуссии в основном носила негативный характер с выраженным недоверием[29].

Как отмечают исследователи, инициативы публичной дипломатии США в странах Ближнего Востока в основном были продиктованы опасениями за имидж США после событий 11 сентября 2001 г. и соображениями национальной безопасности. В таком контексте *война идей* рассматривалась как естественная составная часть *войны против терроризма*. Американский исследователь Джейми Метцл приходит к сходному выводу о том, что использование ИКТ и спутникового телевидения в публичной дипломатии США ставит своей целью «легитимацию использования силы»[30].

Рассмотрев в общих чертах понятие *цифровой дипломатии*, ее историю и ключевые особенности, мы можем попытаться определить, какое влияние программы США в этой области оказывают на современную международную безопасность.

ВЛИЯНИЕ ЦИФРОВОЙ ДИПЛОМАТИИ США НА МЕЖДУНАРОДНУЮ БЕЗОПАСНОСТЬ

В самом широком смысле безопасность определяется как *неугрожаемое состояние*. Долгое время международная безопасность предполагала отсутствие большой войны, а угрозы носили в основном военно-политический характер. Ключевой проблемой представлялась так называемая *дилемма безопасности*, обретающая актуальность в ситуации, когда усиление одного государства в условиях анархичной международной среды вызывает опасения его партнеров. В результате страны вовлекаются в гонку вооружений, следствием чего является конфликтный цикл, как правило, заканчивающийся войной. Ситуация во многом изменилась в XX в. с появлением ядерного оружия, которое сделало невозможной большую войну между сверхдержавами.

Однако в конце XX — начале XXI в. среда международной безопасности снова претерпевает существенные изменения. Как отмечает видный российский ученый В. М. Кулагин, происходит расширение субъектной и предметной сферы международной безопасности[31]. В роли субъектов международной безопасности выступают не только государства, но и новые *актеры* — террористические сети, транснациональные преступные группировки, частные военные компании. Появляются новые невоенные угрозы — экологическая, экономическая и информационная. Для информационной сферы характерна существенная роль негосударственных субъектов, влияющих на безопасность, — в этой связи нельзя не упомянуть угрозы

киберпреступности и кибертерроризма. Представляется, что угрозы, порождаемые программами и инициативами в рамках *цифровой дипломатии*, необходимо рассматривать в общем контексте информационной безопасности.

В исследовательском сообществе нет консенсуса относительно употребления терминов *информационная безопасность* и *кибербезопасность*, что связано с расхождениями в подходах государств к определению угроз в сфере ИКТ, подлежащих урегулированию на международном уровне[32]. Обеспечение *информационно-технической* безопасности включает защиту, контроль и соблюдение законности и правопорядка в телекоммуникационной сфере. В частности, в это понятие входят вопросы защиты от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, *логических бомб*, компьютерных вирусов и вредоносных программ, несанкционированного использования частот, радиоэлектронных атак и т.д.

Обеспечение же информационно-психологической безопасности предполагает защиту психологического состояния общества и государства от негативного информационного воздействия. Российские исследователи и дипломаты-практики склонны придерживаться второго, расширительного подхода, в то время как первый подход применяется в США, странах ЕС и ряде других государств. В данном исследовании в зависимости от контекста будут использоваться оба термина. Вместе с тем основные угрозы безопасности в связи с реализацией программ *цифровой дипломатии* лежат в более широкой плоскости, чем исключительно технологические и программные, поэтому для настоящей работы характерен широкий подход к пониманию информационной безопасности.

Информационная безопасность появилась в международно-политической повестке дня — и, как следствие, в исследовательском и публицистическом дискурсе — после окончания холодной войны в результате изменения геополитической ситуации и информационной революции. Изначально термин *информационная безопасность* использовался в контексте развития ИКТ для обозначения проблем, порождаемых компьютерными сетями. Впоследствии, однако, он приобрел значительно более широкий смысл, выходящий за рамки исключительно технологической сферы.

Лидерство в области изучения проблем кибербезопасности принадлежит исследовательскому сообществу США. Особо следует выделить концепцию *информационных войн второго поколения*, разработанную аналитиками *RAND Corporation*. В соответствии с данной концепцией, информационные атаки рассматриваются как атаки нового типа в рамках стратегического межгосударственного противоборства. В российской исследовательской литературе информационная безопасность рассматривается в контексте так называемой *триады угроз* международной информационной безопасности, которая включает террористическую, военную и криминальную угрозы.

С позиций реалистского направления в теории международных отношений о наличии угрозы международной безопасности говорят в условиях нарушения баланса сил, чрезмерного усиления какого-либо государства, которое другие страны воспринимают как угрозу собственной безопасности. Как правило, ответом становится гонка вооружений и стремление восстановить нарушенное равновесие сил. Таким образом, программы *цифровой дипломатии* США могут представлять угрозу международной безопасности в том случае, если они нарушают баланс сил на международной арене и провоцируют ответную реакцию. На эту опасность обращает внимание, в частности, специальный координатор по вопросам использования ИКТ в политических целях МИД РФ А. В. Крутских. По его словам, «основная озабоченность в сфере обеспечения международной информационной безопасности связана с возможностью применения информационно-коммуникационных

технологий (ИКТ) в целях, несовместимых с задачами обеспечения международной стабильности и безопасности»[33].

Подтверждением тому, что программы *цифровой дипломатии* воспринимаются как угроза на международной арене, служит существующая тенденция к *фрагментации* глобальной информационной сферы, вычленения из нее национальных и региональных сегментов. На неформальном саммите Шанхайской организации сотрудничества (ШОС) в августе 2011 г. обсуждалась возможность введения *информационных границ* с целью оградить государства-участницы от негативных последствий *цифровой дипломатии*.

Показательно, что крупные компании интернет-индустрии зачастую принимают правила игры: *Yahoo!, Google* и другие IT-корпорации сотрудничают с авторитарными правительствами и передают конфиденциальную информацию о своих пользователях, блокируют определенные типы поисковых запросов. После непродолжительного конфликта *Google* с правительством Китая в 2010 г., поводом для которого стали атаки китайских хакеров на корпоративные сети компании и кража персональных данных пользователей ее сервисов, IT-гигант возобновил свою работу на рынке КНР[34]. В этих условиях возникает опасность *фрагментации* интернета, распада его на несколько несвязанных сегментов. Такого рода фрагментация возможна либо за счет формирования закрытых, внутригосударственных *островов* внутри глобальной сети интернета, либо формирования параллельных проектов интернета за счет создания альтернативной системы доменных имен DNS[35].

Результатом нарушения баланса сил также становится гонка вооружений в информационной сфере. Китай еще в 2001 г. заявил о том, что в условиях существенного отрыва Соединенных Штатов в научно-технологической сфере достижение паритета не представляется возможным, и в этих условиях КНР будет ориентироваться на информационные средства воздействия. Все большее число государств вовлекаются в реализацию программ по созданию таких средств воздействия, а также по ведению информационных войн. По данным Главного контрольного управления Конгресса США на 2005 г., более 120 стран занимались разработками в области информационного оружия[36], считая такую деятельность адекватным ответом на свою неспособность поддерживать баланс сил на международной арене. Также в ряде стран сегодня разрабатываются концепции ведения информационных войн и предпринимаются попытки их реализации. Между тем, дальнейшее движение по этому пути может расшатать сложившуюся систему международной безопасности и контроля над вооружениями. Как убедительно показал в своей работе Мартин Либицки, один из признанных классиков теории информационной войны, традиционные меры сдерживания в информационном пространстве малоэффективны вследствие дешевизны и доступности для террористических и преступных группировок информационного оружия, сложности выявления источника угрозы[37].

Информатизация порождает новые угрозы и для государств-лидеров, усиливая *асимметричную* составляющую современных конфликтов, в результате чего уязвимыми оказываются развитые в технологическом плане государства. По мнению ряда исследователей, американская военная мощь и развитие информационного оружия на деле лишь способствовали провоцированию глобальной конфликтности, — в том числе за счет попыток противников США создать ядерное оружие, и ослабили безопасность, для обеспечения которой предназначались[38]. Кроме того, двоякое влияние ИКТ на международную безопасность проявляется, с одной стороны, в их содействии демократизации (что и является их целью в соответствии с официальной позицией США) и, следовательно, снижению конфликтности. С другой стороны, информационные технологии являются удобным инструментом для создания асимметричных угроз и наращивания политического влияния, результатом чего становится провоцирование новых вооруженных столкновений[39].

Несколько иной взгляд на проблему предлагает известный американский политолог и социолог Мануэль Кастельс. По его мнению, появление *цифровой дипломатии* следует рассматривать не как угрозу международной безопасности, а скорее как источник новых возможностей для развития и разрешения современных глобальных проблем, масштаб которых не соизмерим с возможностями и ресурсами отдельно взятого государства. Подобная разница между уровнем проблем и возможностями по их разрешению формирует запрос на *глобальное управление*. Глобальные информационные сети и социальные медиа предлагают возможности для формирования глобального гражданского общества и глобальных дискуссий. Публичная дипломатия в таком контексте рассматривается не как дипломатия государства, но как *народная дипломатия*, которая создает основу для национальной публичной дипломатии и действует *поверх* межгосударственных отношений, основываясь на общих подходах[40].

Действительно, обсуждение внешней политики и глобальных проблем на уровне не только дипломатов, но и рядовых пользователей интернета и мобильных телефонов может способствовать укреплению международной безопасности благодаря формированию атмосферы доверия в международных отношениях. В этом контексте программы *цифровой дипломатии* способствуют формированию единого информационного пространства, глобального гражданского общества, а также складыванию системы управления в мировой политике и разрешения кризисов и проблем, затрагивающих все страны мира.

Однако важно понимать, что все противоречия, которые существуют в межгосударственных отношениях, характерны и для информационной сферы. Как отмечает Кастельс, сегодня в мире наметился новый раунд борьбы за власть в глобальном информационном пространстве. Такой тезис подтверждается многочисленными примерами: систематической цензурой электронной почты в Китае, принятием Евросоюзом законопроектов, направленных на регулирование в области ИКТ, скупки различными игроками сайтов социальных сетей с целью отслеживания их использования и поведения пользователей, выработки и продвижения инициатив, направленных на дифференциацию сетевого трафика, и массой других процессов[41].

Информация на сегодняшний день является ключевым ресурсом *мягкой силы* на международной арене. *Мягкая сила* предполагает использование методов воздействия, ориентированных на коммуникацию. Автор концепции *мягкой силы* Джозеф Най определял ее следующим образом: «*Мягкая сила* — это способность добиваться желаемого за счет добровольного участия союзников, а не с помощью принуждения или подачек»[42]. Най противопоставляет *мягкую силу*, ориентированную на привлекательность страны за счет ее культуры, идеалов или программ, *жесткой силе*, обусловленной военной или экономической мощью нации. В упомянутом труде *Будущее власти* автор приходит к выводу о том, что в эпоху информационной глобализации в международной политике трансформируется само содержание власти, которая опирается уже не на военные, а на информационные ресурсы. «В век информации может победить тот, кто способен представить себя в лучшем свете»[43]. Именно на это направлены программы *цифровой дипломатии* Соединенных Штатов.

Неудивительно, что расширение возможностей США в области глобального информационного влияния за счет использования средств информационного воздействия и *цифровой дипломатии* порождает у менее продвинутых в этой сфере государств ощущение уязвимости и желание отгородиться от глобального информационного пространства, а также создавать собственные информационные средства воздействия, в том числе принимать программы ведения информационных войн. Ситуация усугубляется за счет того, что государства рассматривают программы *цифровой дипломатии* США как попытку вмешательства во внутрен-

ние дела, угрожающую нарушением их государственного суверенитета. Наличие таких опасений подтверждают регулярные попытки закрыть доступ к сервисам *Facebook, YouTube, Blogspot* — в разные периоды времени они были заблокированы во Вьетнаме, Иране, Саудовской Аравии, Египте, Пакистане, Мьянме, Северной Корее и ряде других стран[44].

В этом контексте не столь важно, что именно представляет бо́льшую угрозу для международной безопасности — политика США, направленная на закрепление превосходства в информационной сфере, или ответная реакция авторитарных государств, таких как Китай или Пакистан, которая создает опасность фрагментации глобального информационного пространства. Важно, что оба явления порождаются логикой международной политики в информационной сфере, неизбежной составляющей которой является борьба за лидерство.

Развитие информационных технологий, в том числе социальных сетей, создает новые технологии для реализации внешнеполитических целей, усиления *мягкой* и *жесткой силы* государства. При этом однозначно разделить *мягкую* и *жесткую* силу весьма непросто. Соединенные Штаты стремятся укрепить свое лидерство в глобальном информационном пространстве, однако даже лидеры становятся уязвимы, что лишь усиливает международную нестабильность. С развитием глобальной сети устаревают традиционные механизмы обеспечения международной безопасности и стабилизации международных отношений, а новые, такие как многоуровневая дипломатия и многосторонние партнерства, пока находятся на начальной или ранней стадиях развития.

ЦИФРОВАЯ ДИПЛОМАТИЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО: ВОЗМОЖНОСТИ ДЛЯ РОССИИ

Рассматривать потенциал *цифровой дипломатии* для России необходимо с учетом нынешней роли и потенциала дальнейшего развития информационного сектора для отечественной экономики, национальной безопасности, системы государственного управления. На сегодняшний день РФ является одним из наиболее динамичных и устойчиво растущих IT-рынков в мире[45]. Доля активных пользователей глобальной сети в России на конец 2011 г. составила, по данным Фонда Общественное Мнение (ФОМ), порядка 46 % населения[46]. По данным исследования, проведенного компанией *TNS*, самой посещаемой социальной сетью *Рунета* в 2011 г. стала *ВКонтакте*, куда заходили 12 млн человек в день, на втором месте оказались *Одноклассники* с 7,2 млн человек в день, за ними следует *Мой мир* с 5,3 млн человек. Наиболее быстрыми темпами в том же году росла сеть *Facebook*, ежедневная аудитория которой достигла 1,2 млн человек[47]. Появились первые сайты в кириллическом домене *.рф*, а вклад интернет-сектора в национальную экономику составил порядка 2% от ВВП[48]. Министерство связи и массовых коммуникаций РФ ведет работу над перечнем стратегических компаний российской интернет-индустрии[49]. Рост внимания российского политического руководства к инновационному потенциалу интернета иллюстрирует и тот факт, что к участию в работе Фонда Сколково приглашены главы таких ведущих мировых ИТ-компаний, как *Google, Cisco, Nokia* и *Siemens*.

Высокий приоритет российских национальных интересов в области ИКТ подтверждается продолжающимся ростом масштабов использования интернета, его экономической значимостью, а также процессом формирования электронного правительства. В соответствии с документами Федеральной целевой программы «Электронная Россия» *(2002–2010 гг.)*, развитие ИКТ рассматривается в качестве инструмента повышения конкурентоспособности экономики, расширения возможностей ее интеграции в мировую систему хозяйства, повышения эффективности государственного управления и местного самоуправления[50].

Внимание к инновационному потенциалу интернета иллюстрирует тот факт, что в состав Фонда, ответственного за развитие высокотехнологичного кластера *Сколково*, были включены главы крупнейших мировых ИТ-компаний, в том числе *Cisco* и *Nokia*.

Российские государственные органы также наращивают свое присутствие в интернете. В 2002 г. появился первый сайт президента России, в 2008 г. был запущен президентский видеоблог, а начиная с 2010 г. ведется аккаунт микроблога *Twitter*. Свои сайты на сегодняшний день имеют все федеральные министерства, ведомства и иные органы государственной власти. Министерство иностранных дел РФ предоставляет всем желающим возможность следить за актуальными событиями внешней политики в социальных сетях, в частности используя площадки *Facebook* и *Twitter*.

В то же время, развитие интернета в России и в мире все чаще рассматривается государственными органами сквозь призму вопросов безопасности. В Стратегии национальной безопасности РФ до 2020 г. информационная безопасность рассматривается в качестве одной из важнейших составляющих национальной безопасности страны[51]. Интернет видится в том числе как канал распространения экстремизма и терроризма, навязывания чуждой идеологии и внешнеполитической пропаганды. Примечательный анализ политики российских властей в области регулирования Рунета провел французский исследователь Жюльен Носетти. В соответствии с основным выводом исследования, власти РФ пытаются *фрагментировать* глобальную сеть, чтобы *обособить* ее российскую составляющую. Главным мотивом такой политики служит «стремление к технологической независимости от мировых — и преимущественно американских — игроков в области информационных технологий»[52].

Стоит отметить, что с начала 1990-х гг. РФ регулярно выдвигает инициативы по обеспечению международной информационной безопасности (МИБ). В 2011 г. такие инициативы — за авторством России и ШОС — получили развитие. На сессии Генеральной Ассамблеи ООН российской стороной были представлены концепция Конвенции об обеспечении международной информационной безопасности, а также проект Правил поведения в области обеспечения международной информационной безопасности[53]. К настоящему моменту эти проекты не превратились в акты международного права, однако они отражают магистральный курс России и ее союзников по вопросам обеспечения МИБ и имеют шансы на широкую поддержку на мировой арене.

На фоне активности Российской Федерации в области информационной безопасности есть основания говорить о том, что в настоящее время интернет недостаточно используется российским государством в качестве инструмента внешней политики и дипломатии, средства укрепления *мягкой силы*, повышения привлекательности образа страны. Являясь движущей силой неоднозначных по своей сути процессов глобализации, интернет открывает перед обществом и госструктурами новые перспективы. Глобальная сеть может послужить задаче наращивания Россией своей *мягкой силы* и формированию позитивного образа страны на международной арене, популяризации ее богатого культурного наследия.

Важно помнить, что субъектами глобальной информационной сферы сегодня являются не только государства, но и транснациональные медиакорпорации, организации гражданского общества, сообщества социальных сетей как самостоятельные субъекты, например, сетевое антиглобалистское движение, а также отдельные индивидуумы. Равным образом и в перспективной *цифровой дипломатии* важную роль, помимо госорганов, должны играть как бизнес-структуры, так и организации гражданского общества. В этих условиях в рамках глобальной информационной сферы начинают складываться новые, многоуровневые модели международного

сотрудничества и дипломатии, в которых принимают участие как государства, так и вышеперечисленные *новые* акторы мировой политики. Подобные модели получают распространение в России: так, с 2010 г. проводится ежегодный Российский форум по управлению интернетом, чья площадка объединяет представителей государства, частных экспертов и ключевых игроков *Рунета* и глобальной информационной сферы.

Как представляется, одним из наиболее перспективных направлений российской *цифровой дипломатии* является вовлечение технологического отечественного бизнеса в проекты в сфере публичной дипломатии. Первые шаги на данном направлении уже были сделаны. Успешен опыт поисковой компании *Yandex*, которая сегодня обрабатывает большую часть запросов русскоязычного интернета, социальной сети *ВКонтакте*, популярной не только в России, но и во многих странах зарубежья, включая государства СНГ, Израиль, Германию и США. В последние годы ускорилась интеграция российских интернет-компаний в мировую информационную и инновационную среду. В качестве примеров можно упомянуть создание фонда *DST Global* с глобальной структурой IT-активов, включающей доли в *Facebook, Twitter* и *Zynga*, покупку *ЖивогоЖурнала* компанией *СУП Медиа*, создание офиса *Yandex* в американской Кремниевой долине.

В формирование позитивного образа российской политики и дипломатии весомый вклад вносят телеканалы *Первый канал* и *RT* (бывший *Russia Today*), вещающие также в цифровом пространстве. Уже созданы блоги российских государственных чиновников и дипломатов на русском и английском языках, на порталах государственных органов публикуются открытые данные об их деятельности. Вместе с тем, компании *Рунета* могут быть более активно задействованы в российской *цифровой дипломатии* для популяризации русского языка и культуры, эффективного донесения российского видения международных проблем до глобальной аудитории.

Услуги компаний и сервисов российского сегмента глобальной сети пользуются популярностью у русскоязычного населения независимо от места проживания. Представляется целесообразным создание и продвижение этими компаниями инициатив, направленных на взаимодействие с зарубежными русскоязычными диаспорами, в том числе научными и профессиональными. Возможным вариантом такого взаимодействия могло бы стать создание специального информационного портала, который предоставлял бы актуальную информацию о возможностях сотрудничества русскоязычной научной диаспоры за рубежом с научными институтами в РФ, создавал бы прямые каналы коммуникации и способствовал решению организационных вопросов такого взаимодействия.

Еще одним перспективным направлением развития российской цифровой дипломатии является использование потенциала интернет-краудсорсинга[54]. Как показали результаты проекта *Карта помощи*, созданного для онлайн-координации усилий граждан по преодолению последствий лесных пожаров летом 2010 г.[55], интернет представляет собой важный инструмент так называемого *умного краудсорсинга* и гражданских инициатив, в том числе трансграничных. Такие проекты, как *Карта помощи*, *Карта пожаров* и подобные им ресурсы интернет-краудсорсинга, на интерактивных платформах могут быть организованы с прицелом не только на российскую, но и на глобальную аудиторию, позволяя решать актуальные общественные проблемы, развивать гражданское общество и повышать эффективность взаимодействия власти и государства, формировать позитивный образ страны. Реализация проектов, аналогичных *Карте помощи,* эффективна в социальных сетях, таких как *Вконтакте, Facebook, Twitter*, а также на специализированных платформах типа *Ushahidi*.

В числе возможных вариантов практического применения краудсорсинга для нужд цифровой дипломатии:

- составление интерактивных карт угроз и проблемных объектов, обсуждаемых на высоком уровне;
- создание интерактивных политико-дипломатических сообществ;
- запуск платформ для обмена открытой информацией по *горячим* вопросам и каналов широкого информирования общественности в случае кризисов.

Использование возможностей таких платформ для решения вопросов в рамках дипломатической повестки даст России возможность существенно повысить эффективность и охват своей дипломатии с относительно небольшими, как представляется, затратами.

***

Для эффективного и инновационного развития России необходимы новые внешнеполитические проекты в цифровой сфере, направленные на укрепление *мягкой силы* и развитие науки, технологий и образования. При реализации таких проектов государство должно учитывать не только угрозы, но и возможности, предлагаемые электронной информационной средой. Подобные возможности предоставляет уже наработанный и перспективный инструментарий *цифровой дипломатии*, которая не должна оставаться исключительной прерогативой Соединенных Штатов. Важно понимать, что информационные технологии могут трансформироваться и меняться, но при этом они представляют один из ключевых технологических продуктов сегодняшнего общества, привносящих в глобальный миропорядок все более выраженный элемент сетецентричности. Именно поэтому государственным структурам, в том числе тем, чьи функции связаны с внешнеполитической повесткой, важно не *откладывать их освоение в долгий ящик.*

Согласно распространенной точке зрения, современные достижения ИКТ, в том числе и социальные сети, уже не выйдут из употребления и не исчезнут в процессе развития технологии. При такой постановке проблемы можно либо опасаться утраты возможности управлять их развитием и содержанием, либо признать невозможность жесткого и полного контроля над ними и попытаться мягко направлять протекающие в них процессы в соответствии с собственными интересами[56]. Эти выводы вполне применимы и к российской внешней политике в интернете. Важно попытаться найти баланс между безопасностью и проактивной внешней политикой в информационном пространстве, направленной на укрепление *мягкой силы* и повышение привлекательности России в мире. Необходимо вовлекать в задачи реализации внешнеполитических целей представителей частного сектора и гражданского общества при ведущей и координирующей роли государства. При этом обеспечение информационной безопасности как на национальном, так и на международном уровне остается обязанностью и прерогативой государства.

При подобном понимании задач политики РФ в информационном пространстве *цифровая дипломатия* может стать передовым орудием продвижения наших национальных интересов на мировой арене — при условии инвестирования в нее достаточных интеллектуальных, технологических и организационных ресурсов. Россия имеет такие ресурсы в распоряжении, однако самым дефицитным из них сегодня является время. По этой причине активизация усилий госструктур в рассматриваемой сфере должна рассматриваться в качестве приоритета на самое ближайшее будущее.

Примечания

[1] См. подробнее: Цветкова Н. Программы Web 2.0 в публичной дипломатии США. *США и Канада: Экономика, политика, культура*. 2011. № 3. С. 109–122.

[2] Babst S. NATO's New Public Diplomacy: The Art of Engaging and Influencing. Atlantic-Community. 2009, Febrary 20, http://www.atlantic-community.org/index/articles/view/NATO's_New_Public_Diplomacy%3A_The_Art_of_Engaging_and_Influencing (последнее посещение — 31 августа 2012 г.).

[3] IT Strategic Plan: Fiscal Years 2011–2013 Digital Diplomacy. US Department of State. 2010. September 1, http://www.state.gov/m/irm/rls/148572.htm (последнее посещение — 31 августа 2012 г.).

[4] Цветкова Н. Цит. соч. С. 110.

[5] World Internet Usage and Population Statistics. World Internet Usage Stats. 2011. December 31, www.internetworldstats.com (последнее посещение — 31 августа 2012 г.).

[6] Slaughter A. America's Edge. *Foreign Affairs*. 2009, № 1, January/February, http://www.foreignaffairs.com/articles/63722/anne-marie-slaughter/americas-edge (последнее посещение — 31 августа 2012 г.).

[7] Цветкова Н. Цит. соч. С. 112.

[8] 21st century statecraft. U.S. Department of State. http://www.state.gov/statecraft/overview/index.htm (последнее посещение — 31 августа 2012 г.).

[9] Цветкова Н. Цит. соч. С. 114–116.

[10] Public Diplomacy: Strengthening U.S. Engagement with the World. A Strategic Approach for the 21st Century, 2010, http://www.carlisle.army.mil/DIME/documents/Public%20Diplomacy%20US%20World%20Engagement.pdf (последнее посещение — 31 августа 2012 г.).

[11] Там же.

[12] Khatib L. et al. Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team. Oxford Internet Institute. CDDRL working papers. 2011, № 120, http://uscpublicdiplomacy.org/media/Exploratory_Case_Study_US_Digital_Outreach_Team.pdf (последнее посещение — 31 августа 2012 г.).

[13] Movements.org. http://www.movements.org (последнее посещение — 31 августа 2012 г.).

[14] Khatib L. et al. Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team. Oxford Internet Institute. CDDRL working papers. 2011, № 120, http://uscpublicdiplomacy.org/media/Exploratory_Case_Study_US_Digital_Outreach_Team.pdf (последнее посещение — 31 августа 2012 г.).

[15] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. The White House Official Website. 2011. May, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (последнее посещение — 31 августа 2012 г.).

[16] IT Strategic Plan: Fiscal Years 2011–2013 Digital Diplomacy. U.S. Department of State. 2010, September 1, http://www.state.gov/m/irm/rls/148572.htm (последнее посещение — 31 августа 2012 г.).

[17] Черненко Е. Интернет-протокольная служба Госдепа. *Газета Коммерсантъ*. 2011, 15 сентября, http://www.kommersant.ru/doc/1773567/print (последнее посещение — 31 августа 2012 г.).

См. также:

Tech@State. U.S. Department of State. http://www.state.gov/statecraft/tech/index.htm (последнее посещение — 31 августа 2012 г.).

"Tech@State: Serious Games Conference" Unlocks Human Potential Through Play. Dipnote. U.S. Department of State Official Blog. 2011, June 6, http://blogs.state.gov/index.php/site/entry/techstate_serious_games_conference (последнее посещение — 31 августа 2012 г.).

[18] Department of Defense Strategy for Operating in Cyber Space. U.S. Department of Defense. 2011. July. http://www.defense.gov/news/d20110714cyber.pdf (последнее посещение — 31 августа 2012 г.).

[19] Более подробно о подходах США к военно-стратегическим аспектам безопасности киберпространства см. статью в этом номере *Индекса Безопасности* статью: Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности. *Индекс Безопасности*. 2013. Весна. № 1 (104). С. 65–86.

[20] National security strategy. The White House. 2010, May, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (последнее посещение — 31 августа 2012 г.).

[21] Роговский Е. США: информационное общество. Экономика и политика. М.: Международные отношения, 2008. С. 354.

[22] Более подробно о влиянии социальных сетей на общественно-политические процессы в контексте *Арабской весны*, а также на национальную и международную безопасность см. в настоящем номере *Индекса Безопасности* статью: Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности.

[23] Чернобай А. Роль социальных сетей в мобилизации протестных настроений на Ближнем Востоке и в Северной Африкев в январе-марте 2011 года. *Идеологические аспекты военной безопасности*. 2011, № 1, http://mod.mil.by/iavb/2011n1/9.pdf (последнее посещение — 31 августа 2012 г.).

[24] Росс А., Скотт Б. Социальные СМИ: причина, следствие и реагирование. *Вестник НАТО*. http://www.nato.int/docu/review/2011/Social_Medias/21st-century-statecraft/RU/index.htm (последнее посещение — 31 августа 2012 г.).

[25] См.: J. Nye. The future of power. NY: Public Affairs, 2011. 300 p.

[26] Aday S. et al. Blogs and bullets. New media in contentious politics. United States Institute of Peace. 2010, № 65, http://www.newmediacenter.ru/wp-content/uploads/2011/10/adayetal2010.pdf (последнее посещение — 31 августа 2012 г.).

[27] Civil Movements: The Impact of Facebook and Twitter. — Arab social media report. 2011, May, Vol 1. № 2, http://www.dsg.ae/portals/0/ASMR2.pdf (последнее посещение — 31 августа 2012 г.).

[28] Morozov E. The Digital Dictatorship. *The Wall Street Journal*. 2010, February 20, http://online.wsj.com/article/SB10001424052748703983004575073911147404540.html (последнее посещение — 31 августа 2012 г.).

[29] Khatib L. et al. Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team. Oxford Internet Institute. CDDRL working papers. 2011, January, № 120, http://uscpublicdiplomacy.org/media/Exploratory_Case_Study_US_Digital_Outreach_Team.pdf (последнее посещение — 31 августа 2012 г.).

[30] Цит. по: Khatib L. et al. Public Diplomacy 2.0: An Exploratory Case Study of the US Digital Outreach Team. Oxford Internet Institute. CDDRL working papers. 2011, № 120, http://uscpublicdiplomacy.org/media/Exploratory_Case_Study_US_Digital_Outreach_Team.pdf (последнее посещение — 31 августа 2012 г.).

[31] Кулагин В. Глобальная или мировая безопасность. *Международные процессы.* 2006, № 14. http://www.intertrends.ru/fourteen/004.htm (последнее посещение — 31 августа 2012 г.).

[32] См. подробнее статью в этом номере *Индекса Безопасности:* Демидов О. Обеспечение международной информационной безопасности и российские национальные интересы.

[33] Крутских А. К политико-правовым основаниям глобальной информационной безопасности. Международные процессы. 2007. № 1 (5). http://www.intertrends.ru/thirteen/003.htm (последнее посещение — 31 августа 2012 г.).

[34] См. например: Google возвращается в Китай. *Ведомости*. 2012, 13 января, http://www.vedomosti.ru/tech/news/1473990/konec_bojkotu (последнее посещение — 31 августа 2012 г.).

[35] См.: The future of the internet. A virtual counter-revolution. *The Economist*. 2010, September 2, http://www.economist.com/node/16941635 (последнее посещение — 31 августа 2012 г.).

[36] Крутских А., Сафронова И. Международное сотрудничество в области информационной безопасности. Портал «Информационно-коммуникационные технологии в образовании». http://www.ict.edu.ru/ft/002472/intcoop.pdf (последнее посещение — 31 августа 2012 г.).

[37] См.: Libicki M. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009. http://www.rand.org/pubs/monographs/MG877 (последнее посещение — 31 августа 2012 г.).

[38] Болгов Р. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты): Автореф. дисс. … канд. политол. наук. СПб: СПбГУ, 2010. С. 12.

[39] Там же. С. 13.

[40] Castells M. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. The Annals of the American Academy of Political and Social Science 2008. № 616. http://prtheories.pbworks.com/w/file/fetch/45138545/Castells_2008_The_New_Public_Sphere.pdf (последнее посещение — 31 августа 2012 г.).

[41] Там же.

[42] Nye J. Soft Power: The Means to Success in World Politics. NY: Public Affairs, 2004. 191 p.

[43] Nye J. The future of power. NY, 2011. 300 p.

[44] Freedom on the Net. A Global assessment of Internet and Digital Media. Freedom House. 2009. April 1. http://www.state.gov/documents/organization/135959.pdf (последнее посещение — 31 августа 2012 г.).

[45] Федеральная целевая программа «Электронная Россия (2002–2010 годы)». Юридическая компания «Интернет и право». 2010, 2 марта, http://www.internet-law.ru/intlaw/laws/e-rus.htm (последнее посещение — 31 августа 2012 г.).

[46] Интернет в России. Методика и основные результаты исследования. Фонд Общественное Мнение. Аналитический бюллетень. 2011. Весна. Вып. 33. http://bd.fom.ru/pdf/Internet%20v%20Rossii%20vol%2033%20vesna%202011%20short.pdf (последнее посещение — 31 августа 2012 г.).

[47] Гаврилюк А. За год число пользователей Интернета в России выросло на 14%. RBC Daily. 2011, 10 февраля, http://www.rbcdaily.ru/2011/02/10/media/562949979689739 (последнее посещение — 31 августа 2012 г.).

[48] Россия онлайн: влияние интернета на российскую экономику. Отчет Boston Consulting Group. 2011, 1 мая, http://img.rg.ru/pril/article/48/57/59/000111333.pdf (последнее посещение — 31 августа 2012 г.).

[49] Кошкина Э. Власти РФ возьмут под контроль инвестиции иностранцев в Интернет. Компьюлента. 2009, 9 апреля, http://net.compulenta.ru/417783 (последнее посещение — 31 августа 2012 г.).

[50] Федеральная целевая программа «Электронная Россия (2002–2010 годы)». Утверждена 28.01.2002. Постановление Правительства РФ № 65. http://www.internet-law.ru/intlaw/laws/e-rus.htm (последнее посещение — 31 августа 2012 г.).

[51] Стратегия национальной безопасности Российской Федерации до 2020 года. Министерство иностранных дел Российской Федерации. Официальный сайт. http://www.mid.ru/ns-

osndoc.nsf/0e9272befa34209743256c630042d1aa/8abb3c17eb3d2626c32575b500320ae4?OpenDocument (последнее посещение — 31 августа 2012 г.).

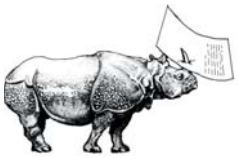
[52] Носетти Д. Кремль «ВКонтакте»: власть и интернет в России. Доклад. Центр Россия/ННГ, апрель 2011 г. http://www.pircenter.org/kosdata/page_doc/p2734_1.pdf (последнее посещение — 31 августа 2012 г.).

[53] См. подробнее статью в этом номере *Индекса Безопасности*: Демидов О. Обеспечение международной информационной безопасности и российские национальные интересы.

[54] Более подробно см. статью в настоящем номере *Индекса Безопасности*: Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности.

[55] Карта помощи пострадавшим от пожаров: Интернет-ресурс. http://www.russian-fires.ru (последнее посещение — 31 августа 2012 г.).

[56] См. например: Lichtenstein J. Digital Diplomacy. *The New York Times Magazine.* 2010. July 16. http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html?pagewanted=all (последнее посещение — 31 августа 2012 г.).



Олег Демидов, Максим Симоненко

ПОЖАР В КИБЕРПРОСТРАНСТВЕ

В конце мая 2012 г. Иран заявил о том, что его нефтяные компании подверглись интенсивным кибератакам. По инициативе Международного союза электросвязи (МСЭ) для расследования этих инцидентов была привлечена российская *Лаборатория Касперского*. Первые технические отчеты об инциденте были опубликованы в понедельник 28 мая того же года. Представители *Лаборатории Касперского* установили, что для осуществления атаки был использован беспрецедентный по сложности *супервирус*, который получил в базе вредоносных программ название *Flame* (англ. *пламя*). Впоследствии оказалось, что венгерская Лаборатория криптографии и системной безопасности (CrySyS) Будапештского университета технологии и экономики с начала мая 2012 г. занималась исследованием вируса, очень похожего на *Flame*, если не идентичного ему.

Первые версии вируса были обнаружены американской компанией *Webroot community* в конце 2007 г. на территории Европы. В следующем году вирус был обнаружен в ОАЭ. Вирусу пришлось проделать длинный технологический и временной путь, чтобы достичь Ирана весной 2010 г. в том виде, в котором его можно было наблюдать в 2012 г. На момент обнаружения в начале мая 2012 г. *Flame* находился на пике своего развития и вошел в фазу максимального распространения. К середине месяца *Flame* распространился по всему ближневосточному региону, так что установить непосредственную цель его создателей стало весьма затруднительно. При создании вируса использовались передовые технологии проникновения в компьютерные системы, но вместе с тем в нем отсутствуют какие-либо эффективные механизмы наведения на конкретную цель. Это позволяет говорить о том, что география распространения *Flame* не отображает спектр и местонахождение конечных объектов, поражение которых являлось его основной задачей.

В равной степени необоснованно выглядит повсеместное использование ярлыка *кибероружия* в отношении *Flame*. Сменщика *Stuxnet* и *Duqu* в галерее главных мировых *киберстрашилок* можно характеризовать по-разному, например, по аналогии с недавним открытием биологов, как *макровирус*, но использование понятия *кибероружие* принципиально искажает суть, назначение программы. В задачи выявленных и описанных модулей не входит выведение из строя компьютерных систем и, тем более, высокоизбирательное физическое поражение объектов критической инфраструктуры, под которое был спроектирован *Stuxnet. Flame* представляет собой эталонное средство ведения затяжного и многоуровневого кибершпионажа. В исследованиях и официальных документах большинства стран с развитым сектором ИКТ кибершпионаж всегда классифицируется отдельно от актов политически мотивированной агрессии в киберпространстве, гипотетических кибервойн

и киберконфликтов, то есть всех тех действий, которые могут осуществляться при помощи *оружия на основе программного кода.*

Навязчивое позиционирование *Flame* в качестве кибероружия, впрочем, кажется отнюдь не случайным — в подаче вируса под таким углом присутствует скрытый логический переход. Согласно последнему, *Flame* внедрялся в сети не в рамках отдельной операции, а скорее как часть стратегии использования обширного киберинструментария, совмещающего средства добычи информации с применением программ, способных наносить непосредственный физический ущерб инфраструктуре. В качестве такой стратегии в первую очередь неявно подразумеваются действия неких субъектов, направленные на торможение ядерной программы Ирана. Действительно, трудно отделаться от впечатления о *комплементарности Flame* и *Stuxnet* — изощренного инструмента выкачивания разнородных данных о любых интересующих объектах и, с другой стороны, хирургически точного орудия их поражения. Проблема, однако, заключается в том, что принимать целеобусловленную связь *Stuxnet* и *Flame* невозможно и контрпродуктивно, а значит, невозможно утвердительно говорить о *Flame* как о кибероружии. Ведь непосредственно кибершпионаж, несмотря на всю свою деструктивную природу, никакого ущерба инфраструктуре не наносит. *Flame* правомерно сравнивать скорее с оптическим прицелом на спайперской винтовке — оказаться в его фокусе весьма неприятно, но убивает все-таки пуля, а не оптика. А в случае с Flame прицел и винтовка существуют вроде как отдельно, и доказать, что они используются совместно, практически невозможно.

В этом контексте любопытна статья *The New York Times* от 1 июня 2012 г.[1], в которой разоблачается санкционированная лично Бараком Обамой грандиозная спецоперация США *Олимпийские игры* по осуществлению серии атак на атомную инфраструктуру Ирана, частью которых якобы стал *Stuxnet*. При всех сенсационных откровениях по поводу *Stuxnet* авторы практически полностью обходят стороной тему *Flame*, хотя сам выход столь подробного материала едва ли случайно столь точно совпал с шумихой вокруг нового супервируса. Попытка лаконично закрыть тему *Flame* ремаркой о том, что его появление не имеет никакого отношения к антииранскому *крестовому походу* США в киберпространстве — и, соответственно, к *Stuxnet*, — оставляет вопросы. Дело в том, что наиболее ценная для NYT целевая аудитория — иранское руководство и экспертное сообщество, не вынесет из статьи ничего принципиально нового по поводу *Stuxnet*. Американо-израильское авторство *Stuxnet* и *Duqu* едва ли ставилось гражданскими и военными экспертами под сомнение. С *Flame* для них все пока не так очевидно, поэтому попытка отвлечь внимание от вопроса, кем создан новый макровирус, могла выглядеть достаточно оправданной, для того чтобы раздувать шумиху вокруг менее актуальной на сегодня угрозы *Stuxnet* за счет громких разоблачений руководства США.

Кроме того, среди захватывающих историй о засекреченной программе *Олимпийских игр* в статье *The New York Times* присутствуют ссылки на факты, которые либо не могут быть проверены при помощи открытых источников, либо в определенной степени противоречат ранее приводившимся фактам о *Stuxnet*. Во-первых, авторы статьи утверждают, что осенью 2010 г., практически сразу после обнаружения *Stuxnet*, вирус поразил от одной до пяти тысяч центрифуг на обогатительных мощностях в Натанзе. Но в начале декабря 2010 г. МАГАТЭ опубликовало отчет о том, что порядка тысячи центрифуг были приостановлены на этом объекте иранской ядерной программы уже в конце 2009 — начале 2010 г. Больше никакой информации о новых остановленных центрифугах не поступало. Во-вторых, в открытых источниках отсутствуют данные, которые бы подтверждали, что центрифугами в Натанзе управляют SCADA производства *Siemens*. Этот момент важен, так как сюжет с SCADA-системами *Siemens* отсылает нас к версии, которую в статье *The New York Times* предпочитают не упоминать, и согласно которой главной целью супервируса была первая иранская АЭС в Бушере. Словом, статья американского издания, предлагая ценные, хотя и неочевидные ответы по поводу *Stuxnet*, ставит лишь новые вопросы в отношении нового шпионского супервируса.

В публикациях СМИ и экспертной среде *Flame* уже стал наиболее комплексной угрозой для информационных систем. И для этого есть основания. Вирус использует последние достижения в области создания вредоносных кодов, а объем вируса, который в совокупности составляет порядка 20 Мб информации и 70 тыс. строк кода, поражает воображение всех специалистов в сфере информационной безопасности. Переходит ли количество в качество? На первый взгляд да. В нем используются современные методы заражения, использующиеся в свое время в *Stuxnet* и *Duqu*: уязвимости в файле автозапуска *autorun.inf*, в файлах типа *.inc*, а также в службе диспетчера очереди печати. Использование этих технологий наталкивает некоторых экспертов на мысль о том, что над разработкой *Flame* и вирусного семейства *Stuxnet* работала одна команда. Но не стоит забывать, что это всего лишь технологии, или кусок кода, который был опубликован в открытом доступе, что позволяет использовать его кому и когда угодно. В добавление ко всему разработчики *Stuxnet* использовали уникальные механизмы маскировки и проникновения вируса — было украдено несколько подлинных цифровых подписей авторитетных производителей компьютерного оборудования, что затрудняло обнаружение вируса антивирусными программами, а также для проникновения в систему использовалась ранее неиспользованная уязвимость нулевого дня. Всего этого нет во *Flame*, в нем используются лишь общедоступные технологии, что может говорить о том, что над *Stuxnet* и *Flame* работали разные команды, хотя не исключено, что действовали они в интересах одного и того же заказчика.

С другой стороны, качество функциональной составляющей вируса не столь очевидно. *Flame* достигает своей громоздкости в первую очередь за счет подключения дополнительных модулей, которые напоминают скорее стандартный *хакерский набор*, чем передовое кибероружие. *Flame* способен собрать любую информацию о компьютере-жертве через перехват сетевого трафика, сбор информации о системе, захват скриншотов определенных процессов и даже запись аудио-разговоров. Но весь этот функционал был уже реализован ранее, только теперь все это собрано в одном месте и сборка различных комбинаций модулей автоматизирована. Такой взгляд на проблему позволяет предположить, что создателем такого супервируса могла выступить даже высококвалифицированная группа *ленивых хакеров*, желающих повысить производительность труда за счет максимальной автоматизации и интеграции своих *бизнес-процессов*. Такое технологическое решение в отношении создания средств кибершпионажа может привести к лавинообразному росту популярности подобных вредоносных продуктов, пусть и менее высокого класса. Сходная ситуация уже имела место в сегменте DDoS-атак. До тех пор, пока для создания ботнетов требовались значительные технологические компетенции и финансовые ресурсы, DDoS-атаки не были широко распространены. Теперь же, когда сформировался развитый рынок аренды ботнетов по доступным ценам, этот вид атак становится очень популярным. Нечто подобное может произойти в сфере вирусописания, когда, для того чтобы достичь своих деструктивных целей в киберпространстве, достаточно будет собрать вирус как конструктор из почти универсальных деталей и модулей.

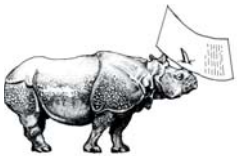
Впрочем, вне зависимости от технологической новизны решений, которые создатели *Flame* заложили в свое детище, перспективы борьбы с супервирусом оставляют довольно грустное впечатление. Основные уязвимости уже латаются, ведущие лаборатории приступили к анализу кода, копии вируса по полученной команде самоудаляются с пораженных систем. Но многомодульные *вирусы* все больше начинают походить на пресловутый кубик Рубика — поворота одной грани, установки одного нового модуля достаточно для того, чтобы программа продолжала функционировать, используя новые уязвимости, список которых никогда не будет исчерпан. Кроме того, международная практика противодействия киберугрозам почти не знает успешных примеров *превентивной* борьбы с созданием и распространением вирусов столь серьезного уровня. Как правило, высококлассные шпионские программы могут успешно функционировать, годами оставаясь незамеченными, а выявляются едва ли не случайно и на той стадии, когда оценить полный объем ущерба и отследить путь вируса уже почти невозможно. При этом

в абсолютном большинстве случаев их обнаруживают частные лаборатории или национальные органы безопасности и правопорядка, никак не связанные с международными структурами. Так было в случаях с *Shady RAT, Moonlight Maze, Titan Rain* и другими высококлассными инструментами кибершпионажа в течение предыдущих лет. В результате налицо выраженный дисбаланс трансграничной природы современных киберугроз и, с другой стороны, преимущественно национальных механизмов поддержания безопасности в Сети. В руках у международного сообщества пока отнюдь не *щит*, способный отражать удары анонимного *кибермеча*, а скорее *пинцет и нитки*, которыми худо-бедно латается нанесенный ущерб.

Между тем вектор, в котором надлежит прикладывать усилия для исправления ситуации, достаточно очевиден и в целом корректно отражен в недавних международно-правовых инициативах РФ, включая концепцию Конвенции об обеспечении международной информационной безопасности. Речь идет, во-первых, о вынесении в политико-дипломатическую плоскость самого понятия *политически мотивированного враждебного поведения в киберпространстве*. Во-вторых, о формировании подлинно глобального режима сотрудничества в области противодействия киберугрозам, прообразом, хотя и не полноценным фундаментом которого можно считать Конвенцию Совета Европы «*О киберпреступности*». Наконец, необходимо четко определить международно-правовой статус киберпространства в контексте национальной и международной безопасности. Для Москвы вопрос заключается в том, удастся ли сдвинуть процесс с мертвой точки раньше, чем новый макровирус изберет целью уже не иранские, а российские сети. Времени не так много.

Примечания

[1] Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all (последнее посещение — 17 августа 2012 г.).



Максим Симоненко

STUXNET И ЯДЕРНОЕ ОБОГАЩЕНИЕ РЕЖИМА МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В центре внимания экспертов и лиц, принимающих решения во многих странах мира, в последнее время оказался вопрос взаимосвязи ядерных и информационных технологий, прежде всего в контексте угроз и вызовов безопасности, внезапно возникших на этом *технологическом перекрестье*. Появление летом 2010 г. компьютерного вируса *Stuxnet*, целью которого, предположительно, являлась ядерная инфраструктура Ирана, резко усилило эту тенденцию. Высказываемые экспертами и СМИ предположения в основном строятся вокруг версии о том, что целью *червя* была автоматизированная система управления технологическим процессом (АСУ ТП) на иранской АЭС в Бушере, а также на обогатительных мощностях в Натанзе.

Однако системы такого типа используются на промышленных объектах самого различного назначения по всему миру: в сетях электропередач, на предприятиях по производству китайских игрушек, в используемых для обогащения урана центрифугах, а технологии управления производственными процессами на разнообразных промышленных объектах ничем принципиально не отличаются друг от друга. Перед экспертным сообществом и политическими управленцами встал вопрос, нужно ли особо выделять безопасность ядерных объектов из прочей промышленной инфраструктуры в смысле обеспечения ее информационной безопасности? От ответа на него зависят национальные и международные политики в части обеспечения информационной безопасности ядерной инфраструктуры — и пока повестка дня в этой сфере выглядит предельно размытой, а международно признанного общего подхода не просматривается.

С другой стороны, в экспертной среде *айтишников* существует убежденность в том, что опыт ядерной эпохи может быть частично применим в целях строительства универсального международного режима информационной безопасности. После обнаружения *Stuxnet* подобные взгляды лишь окрепли. Отнюдь не случайно летом 2012 г. руководитель *Лаборатории Касперского* Е. В. Касперский выступил с идеей создания *киберМАГАТЭ* как некоего межгосударственного механизма, транслирующего опыт работы Международного агентства по атомной энергии (МАГАТЭ) в область информационных технологий. Назначение такого механизма — заложить основы международного режима безопасности киберпространства, основанного на системе мониторинга, взаимных обязательств и призванного не допустить разработку кибероружия и ведение кибервойн.

Такая идея, при всей кажущейся *правильности*, неминуемо провоцирует ряд вопросов. Насколько приемы, методы и стратегические аксиомы теории ядерного сдерживания применимы к киберпространству? Будет ли достаточно для защиты от *Stuxnet* и его аналогов того, что все государства сообща выработают свод норм поведения в киберпространстве и объявят его зоной, свободной от кибероружия?

И возможно ли даже такое взаимодействие, не берущее в расчет негосударственные акторы, сегодня? Ведь, говоря языком метафор, у *здания* международного режима безопасности киберпространства не просто отсутствует фундамент — не утверждено даже *техническое задание* на его строительство и сам его проект. А если ждать, то сколько и чего дожидаться? Ведь сложные вирусы, близкие по уровню к *Stuxnet — Flame, Duqu, Gauss,* уже выявляются раз в несколько месяцев, и никто не знает, когда и с какими последствиями *выстрелит* очередное изощренное кибероружие. Такие вопросы заставляют более подробно и тщательно взглянуть на теперь уже знаменитый вирус, поразивший иранские объекты, чтобы понять, кем и для каких целей он был создан и насколько его реальный *жизненный цикл* совпал с изначальными планами его авторов. Лишь отталкиваясь от знаний об этом, мы можем понять, когда, с кем и какой режим противодействия подобным угрозам необходимо строить, каким содержанием его наполнять и что можно привнести в него от доктрин *ядерной эры*.

STUXNET: *ПРОТИВОЯДЕРНОЕ* КИБЕРОРУЖИЕ

В июне 2010 г. белорусская компания *VirusBlockada*[1], специализирующаяся в области компьютерной безопасности, впервые обнаружила высокотехнологичный компьютерный вирус *RootTmphider* (позднее получивший название *Stuxnet*), направленный против АСУ ТП[2]. К концу 2010 г. в мире уже насчитывалось порядка 100 тыс. компьютеров, зараженных этим вирусом. Наибольшее число заражений было зафиксировано в Иране (58,3 %), Индонезии (17,8 %) и Индии (10 %)[3]. Вместе с тем вирус был обнаружен уже на этапе *разрастания эпидемии*, что не позволяет говорить о том, что страны с наибольшим количеством зараженных компьютерных систем являются первичным очагом распространения вируса[4]. Этот нюанс находит подтверждение в официальной статистике компании производителя АСУ ТП, против которой был направлен вирус, — *Siemens*. Согласно официальному заявлению компании, к марту 2011 г. было обнаружено 24 случая заражений компьютерным вирусом промышленных систем клиентов *Siemens*[5].

Stuxnet, вне сомнений, представляет собой высокотехнологичный продукт, над созданием которого работала достаточно большая и высококлассная команда. В качестве подтверждения обычно упоминается, что при разработке вируса использовались четыре ранее неизвестных уязвимости *нулевого дня*, для маскировки применялись несколько украденных официальных сертификатов крупных производителей компьютерной техники, а также привлекались технические компетенции по производственной эксплуатации АСУ ТП. Все это позволило экспертам и СМИ говорить о том, что автором *Stuxnet* было некое государство или группа государств, а сам вирус был представлен в качестве сверхсовременного силового инструмента реализации национальных интересов.

Согласно такой логике, *Stuxnet* — это *кибероружие*, имеющее колоссальную разрушительную мощь, теоретически сравнимую с оружием массового уничтожения. В середине июня 2012 г. исполнительный директор и издатель *Bulletin of the Atomic Sciences* Кеннет Бенедикт сравнила произведенный *Stuxnet* эффект с первыми ядерными взрывами в Хиросиме и Нагасаки[6]. В то же время при рассмотрении угроз из киберпространства очень часто апеллируют к концепциям эпохи холодной войны — сдерживания и возможности ответного ядерного удара. Такой подход даже нашел отражение в официальной киберстратегии Пентагона, в которой кибератаки приравниваются к традиционным военным действиям, в ответ на которые могут использоваться любые доступные средства вплоть до ядерного оружия[7]. Упомянутое выше предложение главы *Лаборатории Касперского* по созданию *киберМАГАТЭ* нацелено именно на предотвращение милитаризации киберпространства по аналогии с *традиционной* гонкой вооружений. С точки зрения российского эксперта, необходимо не просто создать институт по контролю над кибервооружениями, но по возможности «скопировать международную систему ядерной безопасности и сделать [ее] кальку на киберпространство»[8].

Но если говорить о кибероружии, кто или что является его мишенью? В настоящий момент наибольшее распространение получили две совершенно разные точки зрения на вопрос о целях *Stuxnet*. Первая версия появилась после того, как в августе 2010 г. исходный код вируса стал доступен в интернете[9] и к его изучению присоединился широкий круг экспертов в области информационной безопасности. В середине сентября немецкий специалист в области информационной безопасности Ральф Лангнер предположил, что *Stuxnet* был направлен против какой-то определенной цели[10]. Чуть позднее удалось выявить такую цель — производственную цепочка, которая отвечала за обмен информацией между программируемым логическим контролером марки *SIMATIC S7* и рабочими станциями АСУ ТП *SIMATIC WinCC* фирмы *Siemens.* Тогда же были впервые выдвинуты предположения о том, что основной целью вируса могла быть система управления АЭС в Бушере, и уже после этого появляются первые упоминания о *Stuxnet* в контексте иранской атомной станции в неспециализированных СМИ[11].

После того как информация о вирусе просочилась в масс-медиа, проектный менеджер АЭС в Бушере Махмуд Джафари заявил, что *компьютерный червь* заразил лишь персональные компьютеры работников станции[12]. Однако руководитель Совета по информационным технологиям при Министерстве промышленности Ирана Махмуд Лиайи отметил, что «шпионский червь *Stuxnet* был создан в рамках электронной войны Запада против Ирана»[13]. Фактически никто из чиновников не признал, что вирус предназначался против каких-либо систем управления АЭС, а Лиайи вообще отметил, что *Stuxnet* был не более чем шпионским червем. При этом, однако, Д. О. Рогозин, будучи еще постоянным представителем РФ при НАТО в начале 2011 г., призвал представителей Альянса провести тщательное расследование по поводу *Stuxnet* для недопущения «нового Чернобыля»[14].

Немного позднее, по мере более тщательного изучения исходного кода вируса возникла новая версия о его конечных целях — таковыми, как выяснилось, могли быть обогатительные центрифуги на иранском заводе по обогащению урана в Натанзе[15]. В ноябре 2010 г. аналитики одной из крупнейших компаний в области информационной безопасности *Symantec* обнаружили, что *червь* был направлен не только против конкретной модели АСУ ТП, но и против конкретных высокочастотных преобразователей иранской компании *Fararo Paya* и финской компании *Vacon*[16], производственные мощности которой располагаются в Китае[17].

В свою очередь, эксперты из Института науки и международной безопасности (ISIS) предположили, что высокочастотные преобразователи именно такого типа могли использоваться на площадках по обогащению урана в Натанзе[18]. Согласно отчету ISIS, в конце 2008 — начале 2009 г. по неопределенным причинам в Натанзе сократился объем производства низкообогащенного урана[19]. В качестве основной причины сокращения эксперты Института называли возможные инженерные ошибки, допущенные в процессе расширения производственных мощностей. С мая 2008 по ноябрь 2009 г. количество функционирующих центрифуг в Иране увеличилось с 3 280 до 4 920, а затем сократилось до 3936[20]. Именно это сокращение количества находящихся в строю центрифуг на 984 было списано экспертами ISIS на счет *Stuxnet*.

К концу ноября 2010 г. президент Ирана Махмуд Ахмадинежад подтвердил, что «им [неким субъектам, действующим в интересах Запада] удалось создать проблемы для ограниченного количества наших центрифуг с помощью внедрения программного обеспечения в электронные детали»[21]. Однако Ахмадинежад ничего не сказал ни про Натанз, ни про какой-либо компьютерный вирус. А уже в феврале 2011 г. эксперты ISIS, основываясь на обновленной информации о *Stuxnet*, отказались от своей версии о том, что он мог стать причиной сокращения обогатительных центрифуг в Натанзе, поскольку функция, которая теоретически могла это сделать так и не была активирована[22]. В июне 2011 г. Лангнер пошел еще дальше и выразил сомнение в том, что вирус был вообще направлен против систем управления газовыми центрифугами[23].

Но это не помешало версии о Натанзе получить дальнейшее развитие, и в начале июня 2012 г. в *The New York Times* появилась информация о том, что высокопоставленные чиновники США и Израиля участвовали в подготовке кампании кибератак под названием *Олимпийские игры*, направленных против обогатительных центрифуг в Натанзе, и осуществлены, в том числе, посредством *Stuxnet*[24]. По информации СМИ, «в течение недели [после обнаружения вируса] его новая версия вывела из строя порядка тысячи центрифуг». Похоже, что это единственный факт, который поддается проверке в открытых источниках. Но пока нет никакой информации о том, что осенью 2010 г. в Иране были проблемы с газовыми центрифугами; наоборот, дела там идут неплохо. Так, 15 февраля 2012 г. количество центрифуг в Натанзе было в очередной раз увеличено, причем сразу на треть, до девяти тысяч[25], а к концу лета превысило 10 тыс., поэтому говорить о том, что *Stuxnet* был создан для саботажа обогатительных центрифуг в Натанзе, преждевременно, — или же кибероперация провалилась.

В данном случае уже отработанный способ определения заказчиков кибератаки по цели нападения не работает, поскольку *достоверно* ничего не известно даже о целях вируса. Вместе с тем его технологическая сложность в некоторой степени может быть преувеличена. Так, к примеру, некоторые из уязвимостей якобы *нулевого дня*, использованных при написании *Stuxnet*, на самом деле уже были известны. Согласно вирусному досье компании *Symantec*, уязвимость в файлах с расширением *.lnk* была использована еще в конце 2008 г. в составе другого вируса, а информация об уязвимости в очереди печати была опубликована в журнале по информационной безопасности *Hakin9* еще до ее использования в составе *Stuxnet*[26]. Соответственно, вирусописателям оставалось найти две из четырех использованных *Stuxnet* уязвимостей *нулевого дня*, а оставшиеся две можно было приобрести на черном рынке или найти в специализированной литературе. Подписанные сертификаты производителей компьютерной техники *Realtek Semiconductor Corp* и *JMicron Technology Corp* могли быть похищены с помощью стандартных методов, чему благоприятствует расположение офисов обеих компаний в научном парке Хсинчу (Тайвань)[27]. Для этих целей мог также использоваться *троян Zeus*, который специализируется на хищении банковской информации, но также мог применяться и для хищения подобных сертификатов[28].

Что касается технологических компетенций по эксплуатации АСУ ТП, хорошим источником информации в данном случае могла выступить программа *Национальный испытательный комплекс АСУ ТП США* (NSTB), в рамках которой на протяжении 2003–2009 гг. проводились различные мероприятия по обсуждению угроз информационной безопасности для АСУ ТП. По итогам программы весной 2010 г. был опубликован итоговый доклад с детальным описанием возможных киберугроз для АСУ ТП[29]. Применительно к *Stuxnet* эта программа интересна тем, что в ее рамках в 2008 г. был проведен Саммит по системам автоматического контроля и управления *Siemens*. В ходе саммита Марти Эдвардс из Национальной лабора-

ЛИСТАЯ СТАРЫЕ СТРАНИЦЫ

Ясно, что запретить разработку и использование информационного оружия на нынешнем этапе вряд ли удастся, как это сделано, например, для химического или бактериологического оружия. Понятно также, что ограничить усилия многих стран по формированию единого глобального информационного пространства невозможно. Поэтому развязки возможны только на пути заключения разумных соглашений, опирающихся на международное право и минимизирующих угрозы применения информационного оружия. Такие соглашения, как реальный вклад в международное право, могли бы только укрепить национальную безопасность подписавших их государств. При это может оказаться даже полезным опыт компромиссов и соглашений, накопленный в политике предотвращения ракетно-ядерной войны и установления стратегической стабильности и баланса сил общего назначения в Европе.

Международные вызовы информационной безопасности. М.: ПИР-Центр, 2001.

тории Айдахо и Тодд Стауффер из *Siemens* выступили с докладом и презентацией по возможным уязвимостям АСУ ТП, на которую был направлен *Stuxnet*[30]. Этими наработками могли уже впоследствии воспользоваться создатели вируса.

В таком случае государства могут быть не единственной категорией потенциальных заказчиков и исполнителей *Stuxnet*. А сам *червь* может быть представлен не только как *цифровой Перл Харбор* или *цифровые Хиросима и Нагасаки* — ведь как простой выстрел не всегда является военным актом, так и любое применение кибероружия не может быть приравнено к акту кибервойны. «Кибератака против энергосистем, может быть частью кибервойны, но и может быть и актом кибертерроризма, киберпреступности или даже… кибервандализма. Оценка и категоризация атаки всегда зависит от мотивации ее авторов и ее конкретных обстоятельств»[31].

Одно из наиболее креативных, но наименее обсуждаемых исследований возможных целей и заказчиков *Stuxnet* было подготовлено генеральным директором *Taia Global* Джеффри Карром в 2010 г. специально для хакерской конференции *Black Hat* в Абу-Даби. В качестве основных сценариев в нем рассматривались возможности кибератак против производств по добыче редкоземельных металлов или урановых руд для осуществления корпоративного саботажа с целью дискредитации *Siemens* или для защиты Китаем Малаккского пролива[32]. В первом случаев некая частная компания могла саботировать деятельность на шахтах конкурентов посредством кибератаки, чтобы установить контроль за глобальными поставками редкоземельных металлов.

В случае с добычей урановых руд инициатором кибератаки могла стать одна из экологических неправительственных организаций, известных своим антиядерным настроем и имеющих достаточно большие финансовые возможности (например, *Greenpeace*). В дискредитации авторитета *Siemens* в преддверии заключения соглашения о создании совместного предприятия между *Siemens* и *Росатомом* могла быть заинтересована французская компания *Areva*. Что же касается Малаккского пролива, то он представляет стратегический интерес для Китая в контексте обеспечения национальной энергетической безопасности и международной торговли.

Таким образом, теоретически не только государственные акторы, но и частные компании и неправительственные организации имели как возможности, так и мотивы для создания подобного вируса. Вместе с тем, как было показано выше, ощутимый вклад в обнаружение, изучение и создания средств защиты против *Stuxnet* был сделан негосударственными акторами — антивирусными компаниями, неправительственными организациями, исследовательскими институтами и даже индивидуальными исследователями, поэтому для создания эффективного режима международной информационной безопасности необходимо учитывать как конструктивное, так и деструктивное влияние негосударственных акторов на киберпространство в целом.

УРОКИ *STUXNET* ДЛЯ МЕЖДУНАРОДНОГО СООБЩЕСТВА

Появление *Stuxnet* в значительной степени ускорило процесс *милитаризации киберпространства*. В настоящее время происходит институциональное оформление возможностей использования киберпространства в военных целях. При министерствах обороны ведущих мировых держав создаются *киберотделы*, разрабатываются стратегии поведения в киберпространстве, проводятся масштабные учения армии и силовых структур с имитацией кибервойны. Но уже появились первые подозрения в отношении того, что угроза в отношении информационной безопасности намеренно преувеличивается военными и компаниями по обеспечению информационной безопасности[33]. Для такой оценки имеются определенные основания, но какие же уроки стоит извлечь из появления такого высокотехнологичного вируса?

По мнению старшего научного сотрудника аналитического центра *RAND Corporation* Мартина Либицки, кибероружие имеет свою специфику[34]. Во-первых, оно способно действовать *точечно*, не нарушая функционирование других элементов и систем, внутри всей информационной технологической инфраструктуры, которая включает целые пласты человеческой жизнедеятельности, начиная с автомобилей и заканчивая системами наведения высокоточного оружия. Во-вторых, кибероружие по большому счету является *одноразовым* — единожды использованная уязвимость в информационных системах становится известной, а по прошествии времени специалистам в области информационной безопасности удается ее *закрыть*. В-третьих, очень сложно установить конечного заказчика создания кибероружия. В-четвертых, возможность оценки мощности и деструктивных эффектов кибероружия достаточно затруднена из-за недостатка информации о его конечных целях и, с другой стороны, сложности выработки точных критериев оценки эффекта от его применения.

Наибольший интерес для разработки технических мер по сокращению деструктивных эффектов от использования кибероружия является его *одноразовость*. Но как показал случай с компьютерным вирусом *Flame*, который был обнаружен весной 2012 г. и использовал часть функционала *Stuxnet*[35], кибероружие *само по себе* не одноразово. Очевидно, все большее распространение получает *модульный дизайн* изощренных вредоносных программ, причем во многих случаях отдельные модули могут заимствоваться и использоваться по отдельности, а сами программы обладают большим ресурсом модифицирования. Назвать этот ресурс бесконечным не позволяет лишь ограниченное число уязвимостей *нулевого дня*, которые создателям таких вирусов удается выявить и использовать для атаки целевых систем.

Соответственно, уместней говорить о том, что потенциал каждого конкретного кибероружия может быть сведен к *однократному* применению. Такой результат может быть достигнут за счет эффективного управления информационными системами, которые требуют своевременного обновления и обслуживания. Для этого необходимо развивать средства раннего обнаружения кибератак, совершенствовать существующие подходы к обеспечению информационной безопасности, укреплять сотрудничество между государственными органами и частными компаниями для своевременного обновления программного и аппаратного обеспечения. Целесообразно проанализировать, в какой степени подобные меры были реализованы в рамках действий по нейтрализации *Stuxnet*.

Изначально изучение вируса велось в рамках узкого круга частных лабораторий в области информационной безопасности и Центра реагирования на компьютерные инциденты в сфере систем управления промышленными процессами (ICS-CERT). Эффективность реагирования ICS-CERT на появление такой серьезной угрозы со стороны впоследствии получила не слишком высокую оценку со стороны экспертов в области кибербезопасности. Центр не смог своевременно предоставить операторам промышленных систем никаких конкретных рекомендаций по устранению уязвимостей, использованных вирусом для проникновения в системы управления промышленными объектами[36]. Лишь после того, как исходный код вируса был опубликован в интернете, к его изучению подключились исследовательские институты и частные эксперты. Сразу после этого появились первые версии относительно того, против каких технологических процессов АСУ ТП был направлен вирус, а также против каких объектов он *мог быть* направлен. Поэтому широкое распространение информации о вирусе способствовало, а не препятствовало нейтрализации его последствий.

Антивирусные компании также сделали немало для изучения вируса и создания *заплаток* для операционной системы *Windows*. Первые *дыры* были закрыты уже на следующий месяц после обнаружения вируса, а большая часть уязвимостей была закрыта в течение нескольких последующих месяцев. Вместе с тем именно благодаря антивирусным компаниям и их широкой клиентской базе, расположенной по всему миру, стало возможно отслеживать географическое распростране-

ние вирусной эпидемии. Даже несмотря на то что «любые оценки по уровню зараженности могут строиться только на основании тех данных, которые антивирусные компании получают с клиентских станций, в тех странах, где у этой компании есть клиенты»[37], практически все компании сходились во мнении, что в большей степени заражению были подвержены Иран, Индия и Индонезия. Одна из ведущих компаний в области информационной безопасности *Symantec* опубликовала детальное досье по *Stuxnet*, которое стало хорошим справочным материалом для многих экспертов, пишущих о вирусе.

Но все это было сделано в условиях, когда антивирусные компании из США, России, Белоруссии и прочих стран имели доступ к клиентским станциям в различных странах. Вместе с тем после ситуации с *Stuxnet* Иран активизировал свои усилия по созданию собственного антивируса[38], а в феврале 2012 г. появилась информация о том, что Иран запретил ввоз зарубежной продукции по обеспечению информационной безопасности[39]. Все это может привести к тому, что в дальнейшей перспективе объем технической достоверной информации о вновь обнаруживаемых вредоносных программных продуктах существенно сократится.

В качестве одного из стимулов к международному сотрудничеству в сфере информационной безопасности могут выступить неутешительные результаты тестирования ведущих антивирусов журналом *Global Control*[40]. Согласно исследованию, проведенному в конце мая 2012 г., ни один из популярных антивирусов не смог обнаружить все существующие версии уже известного червя *Stuxnet*[41]. Сможет ли в таком случае отдельная компания, пусть и поддерживаемая государством, обнаружить новые, прежде неизвестные вирусы сходного уровня сложности, или, возможно, еще более скрытные и изощренные? Очень маловероятно. То же самое справедливо и в отношении возможностей отдельно взятых государств по обнаружению подобного рода вредоносных программ и борьбе с ними.

Вместе с тем, для того чтобы устранить уязвимости на аппаратном уровне в АСУ ТП компании *Siemens*, которые были использованы *Stuxnet*, различным компаниям и иранскому правительству потребовалось немногим менее двух лет[42]. Между тем продукт уровня *Stuxnet* при наличии должных человеческих и финансовых ресурсов может быть создан с нуля за несколько месяцев. В данном контексте интерес представляет модель использования открытого аппаратного и программного обеспечения[43] для повышения *скорости устранения* возникающих угроз, что позволит увеличить конкуренцию и инновационный потенциал компаний в сфере информационной безопасности.

В результате проведенного обзора неизбежно возникает вопрос, каким образом версия о том, что *Stuxnet* был направлен против ядерной инфраструктуры, обогатит дискуссию в сфере информационной безопасности. Чем может помочь опыт режима ядерного нераспространения при решении задач обеспечения международной информационной безопасности и противодействия разработке кибероружия, подобного *Stuxnet*?

ЗА РАМКАМИ *STUXNET*: ОПЫТ ЯДЕРНОГО НЕРАСПРОСТРАНЕНИЯ ДЛЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Работа над строительством режима ядерного нераспространения началась практически сразу после первых испытаний атомной бомбы в 1945 г. и велась исключительно узким кругом национальных государств. Такой подход обусловливался в первую очередь крайне высокими экономическими и техническими порогами для создания ядерного оружия (ЯО), преодолеть которые на тот момент были способны лишь передовые державы. Уже в 1946 г. появились первые предложения относительно того, как предотвратить распространение ЯО. В выпущенном в США докладе Ачесона–Лилиенталя содержались предложения поставить под международный контроль все военное направление ядерной деятельности. Для контроля над мирной атомной энергетикой предполагалось ввести механизмы лицензи-

рования и инспекций[44]. В качестве ключевых компонентов распространения ЯО авторы доклада отмечали добычу урановых руд и производство расщепляющихся материалов[45].

К началу 1950-х гг. количество и объем разведанных урановых залежей значительно выросли[46], в результате чего монопольный контроль за ними становился практически невозможнен, поэтому дальнейшие усилия по созданию режима ядерного нераспространения осуществлялись в ключе противодействия распространению технологий производства расщепляющихся материалов оружейного качества. Изначально процесс производства таких материалов был энергоемким и требовал значительных производственных мощностей. Так, к примеру, лаборатория по производству необходимых ядерных материалов в ходе реализации Манхэттенского проекта к 1945 г. потребляла электроэнергии в три раза больше, чем высокоразвитый индустриальный Детройт (США), а в момент наибольшей загруженности на проекте работало порядка 12 тыс. человек[47].

Примерно через десятилетие в СССР появились более простые и дешевые технологии производства ядерных материалов путем обогащения урана в газовых центрифугах. За этим последовало появление целого ряда программ по созданию газовых центрифуг в Израиле и Франции (1960 г.), Китае (1961 г.), Австралии (1965 г.), Швеции (1971 г.), Италии и Индии (1972 г.), Японии (1973 г.) и Бразилии (1979 г.)[48]. Все это привело к тому, что Китай, Франция, Индия, Израиль[49] использовали эти программы для создания ядерного оружия.

Для предотвращения распространения ядерных технологий военного назначения в середине 1950-х гг. было создано Международное агентство по атомной энергии (МАГАТЭ). Предполагалось, что государство, которое хочет использовать мирную атомную энергетику, но не имеет достаточных технологий и компетенций, может получить их у МАГАТЭ. В обмен на это государство должно было заключать соглашение с МАГАТЭ, по которому последнее получало право проведения инспекций на местах для верификации того, что полученные технологии не используются для разработки ядерного оружия. Но неотъемлемой частью любого международного режима, помимо институтов и правил поведения, являются нормы и принципы, в соответствии с которыми выстраиваются взаимодействия между участниками международного общения. Такие нормы и принципы несколько позднее были сформулированы в Договоре о нераспространении ядерного оружия (ДНЯО), который был принят в конце 1960-х гг. А еще позже сформировался механизм экспортного контроля за *чувствительными* технологиями, включая технологии мирного ядерного цикла, которые потенциально могут быть использованы в военных целях.

За последнее десятилетие также был сделан ряд шагов по усилению режима нераспространения. В частности, была принята резолюция ООН № 1540 с призывом к государствам-участникам привести механизмы экспортного контроля на национальном уровне к международным стандартам. Также была принята Инициатива по безопасности в борьбе с распространением оружия массового уничтожения (ИБОР), построен и усилен ряд других финансовых и экспортных режимов.

При рассмотрении этого *краткого резюме* опыта человечества в области ядерного нераспространения возникает закономерное стремление транслировать накопленный опыт на киберпространство и повестку контроля за разработкой кибероружия.

Если при создании ядерной бомбы *точкой отсчета* являются урановые руды, цикл использования которых включает добычу, обработку, обогащение и заканчивается производством ядерной энергии, то для создания кибероружия (информационного по своей природе) такой точкой становятся *сигналы*. Для того чтобы информационные сигналы можно было преобразовать в законченное кибероружие, им потребуется пройти ряд процессов, по смыслу весьма похожих на обогащение урановых руд (см. таблицу)[50].

Изначально получается (добывается) сигнал, выступающий в роли сырья для создания кибероружия. Затем добытое сырье — *данные* — проходят когнитивное структурирование (обработку) и превращаются в *информацию*. Этап адаптации информации к решению конкретной задачи (обогащение) наиболее *чувствителен*, как и в случае с ядерными технологиями, поскольку именно здесь происходит выбор того, как будут использованы полученные знания — в военных или мирных целях. Этот выбор может происходить как внутри какого-либо института, так и внутри человека. Если в рамках организационных структур теоретически возможно создавать внешние механизмы контроля выбора, в какую сторону преобразовывать информацию, то создать подобные механизмы внутри человека технологическими способами невозможно. По сути, кибероружие — это знания, которые были созданы и агрегированы для достижения определенных целей в киберпространстве, но односторонними де-факто *силовыми* средствами. В таком случае запретить производство кибероружия едва ли возможно, поскольку речь фактически будет идти о запрете на производство знаний в условиях информационного общества.

Таблица 1. **Условная схема преобразования сигнала в знания**

Сигналы (фактически сырье) *поступают в аналоговом виде на датчик*
↓
Данные (добытое сырье) *фиксируются в цифровом виде*
↓
Информация (обработанное сырье) *когнитивное структурирование*
↓
Знание (обогащение сырья) *адаптация к решению конкретной задачи*

Поэтому опыт технического контроля над обращением ядерных материалов и технологий лишь в малой степени может быть применим для предотвращения распространения кибероружия. Вместе с тем опыт развития мер доверия, обмена информацией, накопленный в *ядерную* эру, может быть использован либо уже используется для противодействия вызовам международной информационной безопасности. В этом плане интересна работа национальных центров по уменьшению ядерной опасности, использовавшихся для обмена информацией об угрозах. Нечто подобное уже реализовано в рамках правительственных и неправительственных компьютерных групп реагирования на чрезвычайные ситуации. Вместе с тем накопленный опыт контроля над ядерными вооружениями отражает преимущественно двусторонний опыт взаимодействия между СССР (впоследствии РФ) и США. Для создания эффективного режима международной информационной безопасности требуется *многосторонний* формат, поскольку природа киберпространства трансгранична. Если в режиме будут *белые пятна*, он не будет эффективным. Кроме того, опыт ядерного нераспространения также не дает ясных ответов на вопрос о том, как можно включать негосударственных акторов в строительство международного режима безопасности.

Но будет преждевременно говорить о том, что режим ядерного распространения завершил свое формирование и справился со всеми актуальными технологическими вызовами. К примеру, установить полный международный контроль над технологиями обогащения урановых руд так и не удалось до сих пор. Главная причина заключается в том, что в силу своих технических характеристик — компактности, легкости производства невозможности провести границу между военным

и мирным использованием — газовые центрифуги становятся беспрецедентным вызовом для существующих институтов нераспространения[51]. Газовые центрифуги являются неотъемлемым элементом инфраструктуры мирного атома. При этом определить, происходит ли обогащение урана для мирных или военных целей без проведения инспекций на ядерных объектах в существующих условиях практически невозможно. Ярким примером такой проблемы, по иронии судьбы, стал нынешний кризис вокруг ядерной программы того же Ирана, ядром которой является деятельность по обогащению урана, ведущаяся и на пораженных *Stuxnet* мощностях в Натанзе.

Сегодняшняя ситуация вокруг Ирана высвечивает и еще одну принципиально важную тенденцию: мощный импульс развития, который был придан режиму ядерного нераспространения в связи с интенсификацией процесса сокращения стратегически арсеналов двух *ядерных гигантов* в 1990-х гг., постепенно начинает *затухать*[52]. Поэтому сегодня возникает потребность в выработке новых мер для дальнейшего развития режима нераспространения, в том числе ядерного разоружения уже на многосторонней основе[53]. Но, как это чаще всего бывает, то, что работает для двоих, не всегда работает должным образом для пятерых и уж тем более для девяти участников. Будет необходимо вырабатывать новые способы верификации соблюдения многосторонних договоренностей как в области более *глубокого* разоружения, так и по вопросам всеобъемлющего запрета ядерных испытаний и производства расщепляющихся материалов для военных целей.

Таким образом, можно увидеть общие проблемные точки как у уже существующего режима ядерного нераспространения, так и у еще не созданного режима международной информационной безопасности. К их числу следует отнести необходимость выработки *социальных* методов предотвращения распространения ядерного и кибернетического оружия, а также потребность в создании многостороннего (а возможно и *многосубъектного*, с участием негосударственных акторов) формата по контролю над вооружениями. Поэтому было бы вполне логично объединить усилия из сообществ *ядерщиков* и *айтишников* для нахождения совместных решений описанных проблем. Начать можно, к примеру, с поиска ответов на вопрос о том, как объекты гражданской ядерной инфраструктуры могут быть вписаны в международный режим информационной безопасности.

В отношении объектов гражданской ядерной инфраструктуры актуальны два направления деятельности, которую в общем справедливо охарактеризовать как обеспечение информационной безопасности:

- с одной стороны, информационная безопасность как таковая (предотвращение распространения чувствительной информации);
- с другой стороны, физическая безопасность, то есть устойчивость функционирования процессов работы с ядерным материалом и прочие элементы информационных систем по обеспечению безопасности объектов[54].

К объектам гражданской ядерной инфраструктуры можно отнести обогатительные мощности, лаборатории и исследовательские институты, исследовательские реакторы и АЭС. Сбои в обеспечении информационной безопасности на таких объектах могут привести, во-первых, к распространению чувствительной ядерной информации, а во-вторых, к недопустимым социальным последствиям. В тех странах, где доля атомной энергии в общем национальном энергобалансе достаточно высока (Франция, Япония, Украина, Германия и др.), речь может идти о негативных экономических эффектах, а также о снижении уровня доверия населения к атомной энергии[55].

На объектах гражданской ядерной инфраструктуры для обеспечения информационной безопасности используется общий для всей сферы ИКТ стандарт ISO 17799 (2000). С 2005 г. была разработана серия обновленных стандартов ISO/IEC 27000, которые получили позитивную оценку МАГАТЭ и будут использо-

ваться при разработке принципов информационной безопасности на объектах мирной гражданской ядерной инфраструктуры. Также в настоящий момент разрабатывается новый стандарт в рамках Международной электротехнической комиссии (МЭК) IEC 62645. Но вместе с тем эти стандарты не учитывают специфику ядерной отрасли по следующим параметрам, которые в первую очередь касаются вопросов физической ядерной безопасности[56]:

- *жизненный цикл* объектов гражданской ядерной инфраструктуры, в котором на каждом этапе подходы к обеспечению информационной безопасности могут различаться;
- *большая требовательность АСУ ТП*, использующихся на ядерных объектах, к точности вычислений, устойчивости работы по сравнению с другими ИТ-системами;
- *наличие удаленных центров управления*, которые в случае чрезвычайной ситуации позволят сохранить контроль за ядерными объектами, что требует создания дополнительных коммуникационных каналов, которые могут быть использованы злоумышленниками;
- необходимость *разработки проверенных процедур обновления программного обеспечения*;
- отработка *процедур закупки качественной компьютерной техники* (без каких-либо закладок или *черных ходов* для получения несанкционированного доступа к компьютерным системам);
- включение *условий в контракты по выполнению работ на субподряде* по недопущению компрометации компьютерных систем со стороны третьих лиц.

Поэтому в 2011 г. в рамках Технической рабочей группы МАГАТЭ по контрольно-измерительным системам АЭС (TWG-NPPIC) была запущена Координированная исследовательская программа (CRP) по безопасности цифровых контрольно-измерительных систем. В рамках инициативы МАГАТЭ было выпущено несколько технических руководств по информационной безопасности, в текущем году планируется публикация более широкого и обзорного доклада *Technical Challenges and Solutions in Application of Digital I&C Systems in NPP.*

Но, как уже отмечалось ранее, одних технологических методов предотвращения киберугроз будет недостаточно, поэтому необходимо развивать международное сотрудничество в этой сфере. Первые шаги в этом направлении были сделаны уже в этом году. В итоговое коммюнике Сеульского саммита по ядерной безопасности в марте 2012 г. вошел раздел, посвященный информационной безопасности на ядерных объектах. Основной акцент в документе делается на меры по предотвращению распространения чувствительной ядерной информации, тогда как проблемы информационной безопасности на уровне физической ядерной безопасности не затрагиваются. Об этом можно судить по тому, что в разделе по информационной безопасности делаются ссылки на резолюцию Генеральной конференции МАГАТЭ по ядерной безопасности GC (55)/Res/10 и резолюцию Международного союза электросвязи № 174[57], которые посвящены сугубо вопросам безопасности чувствительной информации. Это предположение также находит подтверждение в презентации представителя посольства Великобритании[58] в США Кейна Полларда на конференции PONI Spring Conference в апреле 2012 г. [59].

МАГАТЭ, в свою очередь, оценивает такой характер угроз для элементов гражданской ядерной инфраструктуры как низкий или средний[60]. А источники угроз, представляющие наибольшую опасность для ядерных объектов и располагающиеся на уровне физической ядерной безопасности, не вошли в раздел итогового коммюнике по информационной безопасности. Поэтому необходимо учесть это обстоятельство и привлечь к нему внимание мирового сообщества. Одной из под-

ходящих для этого площадок видится предстоящий в 2014 г. Саммит по ядерной безопасности в Нидерландах.

С другой стороны, возникает не менее важный вопрос о том, каким образом гарантии безопасности для объектов гражданской ядерной инфраструктуры могут быть *инкорпорированы* в международный режим информационной безопасности? Для поиска ответа на этот вопрос требуется более широкое обсуждение проблематики среди экспертов в сфере ядерных и информационных технологий. Изначально это может быть сделано на какой-либо разовой площадке, но впоследствии может потребоваться более тесное сотрудничество между представителями обеих сфер, а также полноценная институционализация такого взаимодействия. По этому пути уже пошли США, где в начале 2009 г. в рамках Министерства обороны был создан Отдел заместителя министра обороны по глобальным стратегическим вопросам. В повестку новой структуры вошли задачи по выработке политики в сфере предотвращения распространения оружия массового поражения, обеспечения ядерной и информационной безопасности, а также решении вопросов, связанных с космосом. Такой опыт релевантен и для России; кроме того, со временем он может быть опробован и на международном уровне, к чему российскому руководству стоит приложить активные усилия.

ЗАКЛЮЧЕНИЕ

Stuxnet вывел целый ряд проблем и сюжетов на авансцену международной дискуссии о будущем режима МИБ и взаимосвязи цифровых и ядерных технологий. Во-первых, *червь* показал, что вопросы создания сколь угодно сложных вредоносных программ, равно как и задачи борьбы с ними, решаются не только силами государств и требуют вовлечения негосударственных акторов. Как дает понять анализ, возможности и мотивы для создания *Stuxnet*, наряду с государствами, имели частные компании, а коммерческие лаборатории сыграли ключевую роль в борьбе с ним. Отсюда вытекает первый вывод: для создания эффективного режима международной информационной безопасности необходимо учитывать разнонаправленное (конструктивное и деструктивное) влияние негосударственных акторов на весь процесс разработки кибероружия и средств защиты от него. Этот фактор обусловливает принципиальное отличие будущих режимов информационной безопасности и контроля над кибероружием от режима контроля над ядерными вооружениями, в которых роль негосударственных акторов была и остается скорее маргинальной.

Второе отличие заключается в диаметрально противоположном сочетании свойств *потенциала применения* и *авторства* ядерного и кибероружия. Ядерное оружие всегда рассматривалось как средство однократного применения, при этом по умолчанию подразумевалась полная ясность относительно того, кто владеет им и применяет его. Без четкой и однозначной атрибуции ядерных арсеналов были бы невозможны любые варианты сдерживания. В случае со *Stuxnet* Иран и другие страны столкнулись с нерешенной проблемой атрибуции, когда подозрения в отношении США и Израиля не могут быть доказаны, а круг потенциальных агрессоров практически неограничен. При этом модификации и переработанные версии вируса едва ли не до сих пор продолжают поражать компьютерные сети в различных странах, а модульный принцип написания превращает кибероружие в *гидру,* способную вновь и вновь поражать системы, находя новые уязвимости и меняя используемые модули. Подобные различия делают идеи прямой *репликации* механизмов ядерного нераспространения и контроля кибертехнологий (*киберМАГАТЭ* Е. В. Касперского) в значительной степени условными.

В то же время понятно, что перспективный режим МИБ должен быть сфокусирован на цели снижения потенциала каждого конкретного кибероружия до *однократного* применения. Затянувшаяся борьба со *Stuxnet* выявила острую потребность в международных механизмах раннего обнаружения кибератак, системах глобального информирования о киберугрозах, привлечении частных компаний для

борьбы с кибероружием в рамках централизованных международных площадок типа ООН.

Однако кейс *Stuxnet* доказывает, что у режима ядерного нераспространения и у перспективного режима МИБ имеются принципиально общие моменты. К их числу относится потребность в *многостороннем* формате обоих режимов. По мере *диффузии* и удешевления атомных технологий снижаются барьеры реализации ядерных программ, вопросы нераспространения и контроля над ядерными вооружениями с новой остротой встают перед *ядерным клубом,* тщащимся сдержать импульс *ядерной пролиферации*. В этих условиях диалог по военным ядерным вопросам, некогда бывший скорее эксклюзивным правом двух сверхдержав и их союзников, превращается в многостороннюю дискуссию, где голос каждой страны имеет вес. Та же ситуация еще более четко прослеживается в сфере информационной безопасности, так как более половины стран мира обладают возможностями по развитию кибервооружений. Таким образом, опыт ядерного нераспространения, не имея параллелей с режимом МИБ в части *многосубъектности*, представляет ценный багаж в плане согласования *многосторонних* решений и подходов различных стран.

Кроме того, опыт контроля над вооружениями может использоваться для развития *социальных механизмов* обеспечения МИБ, то есть предотвращения утечек чувствительных знаний о программных разработках и системах защиты, по аналогии с *ядерным знанием*. Сегодня импульс ядерного нераспространения начинает несколько ослабевать, а сам режим находится на том рубеже, когда требуется создать и запустить новые механизмы для его дальнейшего развития. При этом частичная схожесть проблем в сферах ядерных и информационных технологий позволяет предположить, что взаимодействие экспертов из обеих областей повысит эффективность находимых решений и позволит достичь *синергии* в преодолении вызовов ядерной и информационной безопасности. В числе перспективных институциональных площадок для такого взаимодействия — Саммит по ядерной безопасности 2014 г. в Нидерландах и другие подобные мероприятия.

Наконец еще одной темой для обсуждения должно стать обеспечение гарантий безопасности объектов гражданской ядерной инфраструктуры в рамках режима МИБ. В силу ряда особенностей, выделяющих ядерные объекты на фоне прочей критической инфраструктуры, — что, опять же, проиллюстрировал *Stuxnet*, — этот вопрос должен получить отдельную нишу в рамках международного режима информационной безопасности. России стоит присмотреться к опыту других стран и начать собственное движение в этом направлении, создавая постоянные структуры, отвечающие за информационную безопасность обширной ядерной инфраструктуры страны.

КОММЕНТАРИИ

Примечания

[1] *VirusBlockada* также имеет офис в Москве и соответствующие лицензии на деятельность по защите конфиденциальной информации от ФСТЭК. См.: ВирусБлокАда. Официальный вебсайт. http://www.virusblokada.ru/about/(последнее посещение — 31 августа 2012 г.).

[2] Falliere N., Murchu L., Chien E. W32.Stuxnet Dossier, V1.4. Symantec. February. 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (последнее посещение — 31 августа 2012 г.).

[3] Там же.

[4] Гостев А. Мирт и гуава: Эпидемия в динамике. 2010. http://www.securelist.com/ru/blog/34361/Mirt_i_guava_Epidemiya_v_dinamike (последнее посещение — 31 августа 2012 г.).

[5] SIMATIC PCS 7: Information about Malware. Handling Stuxnet. *Siemens International.* http://support.automation.siemens.com/WW/adsearch/resultset.aspx?region=WW&lang=en&ne

tmode=internet&ui=NDAwMDAxNwAA&term=stuxnet&ID=43876783&ehbid=43876783 (последнее посещение — 31 августа 2012 г.).

[6] Benedict K. Stuxnet and the Bomb. *The Bulletin*. 2012. June 15. http://thebulletin.org/web-edition/columnists/kennette-benedict/stuxnet-and-the-bomb (последнее посещение — 31 августа 2012 г.).

[7] Department of Defense Strategy for Operating in Cyberspace. U. S. Department of Defense. July 2011. http://www.defense.gov/news/d20110714cyber.pdf (последнее посещение — 31 августа 2012 г.).

[8] Касперский Е. Net voine! Nota Bene. Евгений Касперский об интересном, приятном и наболевшем. 2011. 21 ноября. http://eugene.kaspersky.ru/2011/11/25/net-voine/(последнее посещение — 31 августа 2012 г.).

[9] Our Stuxnet timeline. Langner. 2010, December 9, http://www.langner.com/en/2010/12/09/our-stuxnet-timeline/(последнее посещение — 31 августа 2012 г.).

[10] Langner R. Stuxnet is a directed attack — 'hack of the century. 2010, September 13, http://www.langner.com/en/2010/09/13/stuxnet-is-a-directed-attack-hack-of-the-century/(последнее посещение — 31 августа 2012 г.).

[11] Автор искал информацию по запросам «*stuxnet*» и «*stuxnet bushehr*» (использовались первые 100 результатов вывода поиска) в поисковой системе *Google Статистика поиска* за периоды с 1 сентября 2010 г. по 20 сентября 2010 г. и с 21 сентября 2010 г. по 21 октября 2011 г. Количество упоминаний *Stuxnet* начинает расти именно с 21 сентября 2010 г.

[12] Stuxnet worm hits Iran nuclear plant staff computers. *BBC*. 2010, September 26, http://www.bbc.co.uk/news/world-middle-east-11414483 (последнее посещение — 31 августа 2012 г.).

[13] Hafezi P. Iran says Bushehr nuclear plant not damaged by Stuxnet. *Reuters*. 2010, September 27, http://www.reuters.com/article/2010/09/27/us-iran-cyber-bushehr-idUSTRE68Q39Z20100927 (последнее посещение — 31 августа 2012 г.).

[14] Brunnstrom D., Ireland L. Russia says Stuxnet could have caused new Chernobyl. *Reuters*. 2011, January 26, http://www.reuters.com/article/2011/01/26/us-iran-nuclear-russia-idUSTRE70P6WS20110126 (последнее посещение — 31 августа 2012 г.).

[15] Melman Y. Computer virus in Iran actually targeted larger nuclear facility. Haaretz. 2010. September 28. http://www.haaretz.com/print-edition/news/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052 (последнее посещение — 31 августа 2012 г.).

[16] Falliere N., Murchu L. O., Chien E. Op. Cit.

[17] Carr J. Stuxnet's Finnish-Chinese Connection. Forbes. 2010, December 14, http://www.forbes.com/sites/firewall/2010/12/14/stuxnets-finnish-chinese-connection/(последнее посещение — 31 августа 2012 г.).

[18] Albright D., Brannan P., Walrond C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment. ISIS. 2010. December 22. http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant (последнее посещение — 31 августа 2012 г.).

[19] Albright D., Walrond C. Iran's Gas Centrifuge Program: Taking Stock. ISIS. 2010, February 11, http://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock (последнее посещение — 31 августа 2012 г.).

[20] Там же.

[21] Hafezi P. Iran admits cyber attack on nuclear plants. *Reuters*. 2010, November 29, http://www.reuters.com/article/2010/11/29/us-iran-idUSTRE6AS4MU20101129 (последнее посещение — 31 августа 2012 г.).

[22] Albright D., Brannan P., Walrond C. Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report. ISIS. 2011. February 15. http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/(последнее посещение — 31 августа 2012 г.).

[23] Langner R. Enumerating Stuxnet's exploits. 2011, June 7, http://www.langner.com/en/2011/06/07/enumerating-stuxnet%E2%80%99s-exploits/(последнее посещение — 31 августа 2012 г.).

[24] Sanger D. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*. 2012. June 1. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all (последнее посещение — 31 августа 2012 г.).

[25] Иран увеличил число центрифуг по обогащению урана в Натанзе до 9 тысяч. *UkraNews*. 2012. 15 февраля. http://ukranews.com/ru/news/world/2012/02/15/64131 (последнее посещение — 31 августа 2012 г.).

[26] Falliere N., Murchu L. O., Chien E. Op. Cit.

[27] Matrosov A., Rodionov E., Harley D., Malcho J. Stuxnet Under the Microscope Revision 1.1. ESET. 2010. http://eset.ru/.company/.viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf (последнее посещение — 31 августа 2012 г.).

[28] Там же.

[29] NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses. DOE Idaho Operations Office. May 2010. http://www.fas.org/sgp/eprint/nstb.pdf (последнее посещение — 31 августа 2012 г.).

[30] Edwards M., Stauffer T. Control System Security Assessments. 2008 Siemens Automation Summit. http://graphics8.nytimes.com/packages/pdf/science/NSTB.pdf (последнее посещение — 31 августа 2012 г.).

[31] Schneier B. Cyberwar. 2007, June 4, http://www.schneier.com/blog/archives/2007/06/cyberwar.html (последнее посещение — 31 августа 2012 г.).

[32] Carr J. Dragons, Tigers, Pearls, and Yellowcake: 4 Stuxnet Targeting Scenarios. 2010, November 16, http://nanojv.files.wordpress.com/2011/03/dragons_whitepaper_updated1.pdf (последнее посещение — 31 августа 2012 г.).

[33] Brito J., Watkins T. Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Mercatus Center at George Mason University. April 2011. http://jerrybrito.com/pdf/3HNSJ39.pdf (последнее посещение — 31 августа 2012 г.).

[34] Libicki M. «Pulling Punches in Cyberspace» in Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U. S. Policy. National Academy of Sciences. 2010. http://www.nap.edu/openbook.php?record_id=12997&page=123 (последнее посещение — 31 августа 2012 г.).

[35] Подробнее см. комментарий в этом номере *Индекса Безопасности*: Демидов О., Симоненко М. Пожар в киберпространстве. С. 229–232.

[36] Peterson D. ICS-CERT: Stuxnet Lessons Learned. *Digital Bond*. 2010. http://www.digitalbond.com/2010/10/22/ics-cert-stuxnet-lessons-learned/(последнее посещение — 31 августа 2012 г.).

[37] Гостев А. Мирт и гуава: Эпидемия в динамике. 2010. http://www.securelist.com/ru/blog/34361/Mirt_i_guava_Epidemiya_v_dinamike (последнее посещение — 31 августа 2012 г.).

[38] Isayev S., Jafarov T. Iran starts making own anti-virus software. *Trend*. 2012, May 3, http://en.trend.az/regions/iran/2021650.html (последнее посещение — 31 августа 2012 г.).

[39] Isayev S., Jafarov T. Iran bans import of foreign computer security software. *Trend*. 2012, February 20, http://en.trend.az/regions/iran/1994160.html (последнее посещение — 31 августа 2012 г.).

[40] Журнал *Control Global* — одно из авторитетных изданий, специализирующихся на глобальных рынках автоматизации промышленных процессов.

[41] What's the Best Defense Against Stuxnet? A Comparison of Which Tools Are the Best for Finding Stuxnet in a System. 2012, May 28, http://www.controlglobal.com/articles/2012/stuxnet-iranian-view.html?page=full (последнее посещение — 31 августа 2012 г.).

[42] Peterson D. Stuxnet Clock Stops At 625 Days. *Digital Bond*. 2012, May 31, http://www.digitalbond.com/2012/05/31/stuxnet-clock-stops-at-625-days/(последнее посещение — 31 августа 2012 г.).

[43] Кларк У., Левин П. Обеспечение безопасности информационной магистрали. *Россия в глобальной политике.* 2010, № 3. http://www.globalaffairs.ru/numbers/74 (последнее посещение — 31 августа 2012 г.).

[44] The Acheson-Lilienthal Report: Report on the International Control of Atomic Energy. Washington, D. C.: U. S. Government Printing Office, 1946. http://www.learnworld.com/ZNW/LWText.Acheson-Lilienthal.html (последнее посещение — 31 августа 2012 г.).

[45] Там же.

[46] NPT Briefing book. Centre for Science & Security Studies, James Martin Center for Nonproliferation Studies. Monterey Institute of International Studies. 2012. http://www.kcl.ac.uk/sspp/departments/warstudies/research/groups/csss/2012nptbook.pdf (последнее посещение — 20 августа 2012 г.).

[47] AEC Handbook on Oak Ridge. Oak Ridge National Laboratory, 1955.

[48] Kemp R. Centrifuges: A new era for nuclear proliferation Nonproliferation Policy Education Center Monograph, 2012. http://npolicy.org/article_file/Centrifuges_A_new_era_for_nuclear_proliferation.pdf (последнее посещение — 31 августа 2012 г.).

[49] По сегодняшний день официальный Тель-Авив не подтверждает и не опровергает информацию о наличии у него военной ядерной программы. Официально Израиль не является членом *ядерного клуба*.

[50] Rowley J. The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science*. 2007. No 33. C. 163–180. http://jis.sagepub.com/content/33/2/163.abstract (последнее посещение — 31 августа 2012 г.).

[51] Kemp R. Centrifuges: A new era for nuclear proliferation Nonproliferation Policy Education Center Monograph, 2012. http://npolicy.org/article_file/Centrifuges_A_new_era_for_nuclear_proliferation.pdf (последнее посещение — 31 августа 2012 г.).

[52] Acton J. Low Numbers: A Practical Path to Deep Nuclear Reductions. Carnegie Endowment for International Peace, 2011. http://carnegieendowment.org/files/low_numbers.pdf (последнее посещение — 31 августа 2012 г.).

[53] Лавров С. Новый договор о СНВ в матрице глобальной безопасности. *Международная жизнь*. 2010. № 7, июль.

[54] За основу взята классификация технического руководства МАГАТЭ *Computer Security at Nuclear Facilities*, выпущенного в 2011 г. Для целей настоящей статьи классификация была упрощена и адаптирована.

[55] Announcement of a new IAEA Co-ordinated Research Programme (CRP). IAEA. 2011. http://www.iaea.org/NuclearPower/Downloads/Engineering/meetings/2011-05-TWG-NPPIC/CRP-CyberSecurity.pdf (последнее посещение — 31 августа 2012 г.).

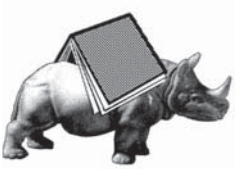
[56] Computer Security at Nuclear Facilities. IAEA Nuclear Security Series No. 17, 2011. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf (последнее посещение — 31 августа 2012 г.).

[57] Seoul Communique. Seoul Nuclear Security Summit, 2012. http://www.thenuclearsecuritysummit.org/userfiles/Seoul%20Communique_FINAL.pdf (последнее посещение — 31 августа 2012 г.).

[58] Великобритания является автором предложений по включению раздела по информационной безопасности в итоговое коммюнике Саммита по ядерной безопасности в Сеуле в 2012 г.

[59] Pollard K. The UK Contribution to the 2012 Nuclear Security Summit. British Embassy in Washington D. C. 2012. https://csis.org/images/stories/poni/120417_Pollard.pdf (последнее посещение — 31 августа 2012 г.).

[60] Computer Security at Nuclear Facilities. IAEA Nuclear Security Series No. 17, 2011. http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf (последнее посещение — 31 августа 2012 г.).



КИБЕРВОЙНА И КИБЕРМИР РИЧАРДА КЛАРКА

Cyberwar. The Next Threat to National Security and What to Do About It. By Richard A. Clarke and Robert K. Knake. Ecco. 290 p.

Рецензия — Олег Демидов

Ричард Алан Кларк проработал с госструктурах США ни много ни мало 30 лет, с 1973 по 2003 г. — сначала в Пентагоне и Госдепартаменте США, а позже в Совете национальной безопасности США. На последнем месте службы он в разное время занимал должности руководителя Группы по обеспечению контртеррористической безопасности, специального советника и, при администрациях Билла Клинтона и Джорджа Буша-младшего с 1998 по 2001 г., пост Национального координатора по безопасности, защите инфраструктуры и контртерроризму. На посту Национального координатора особое внимание г-н Кларк уделял кибербезопасности, включая проблемы кибершпионажа и конфликтов в киберпространстве. Затем, в силу глубоких разногласий с курсом Буша в сфере национальной безопасности, ушел, как водится, в частный сектор. А в 2010 г., в соавторстве с молодым исследователем Робертом Кнейком, написал книгу *Кибервойна. Новая угроза национальной безопасности и пути ее преодоления*, вложив в нее весь свой опыт и все знания, приобретенные за долгие годы госслужбы.

То, что получилось, можно назвать одной из наиболее системных, всеобъемлющих и практических публикаций на тему военно-политического значения киберпространства, в первую очередь для США. Книга идеальна для тех, кто желает вникнуть в проблематику кибервойн на серьезном уровне с нуля, не будучи специалистом в этой области. Авторам удается сочетать доступную и легкую манеру изложения с въедливым анализом нынешней ситуации и богатейшей фактурой. Место находится даже элементам академической теории, вплетаемым в рассуждения о сходстве нынешней эпохи с 1950-ми гг., когда военный атом, так же, как и кибероружие сегодня, поставил мир перед задачей выработать режим его контроля во избежание глобальной катастрофы.

Кларк показывает проблему в полном ракурсе, начиная с описания того, что такое кибервойна, насколько она реальна и какие события в недавнем прошлом можно считать ее первыми прецедентами. Стоит ли отсчитывать ее историю от кибератак против государственной и коммерческой инфраструктуры Эстонии, сопутствовавших скандалу вокруг *Бронзового солдата* в 2007 г.? Или от подобных, но еще более масштабных атак на инфраструктуру Грузии, впервые происходивших параллельно с военным конфликтом — *Пятидневной войной* в августе 2008 г.? А что, если понятие кибервойны подразумевает поражение военных систем, напрямую влияющее на *оффлайновое* пространство боевых действий? В таком случае счетчик истории кибервойн возвращает нас в 2007 г. к операции *Фруктовый сад*, когда бомбардировке сирийского объекта, предположительно связанного с подпольной ядерной программой, предшествовал взлом систем ПВО Сирии при помощи компьютерной программы *Senior Suter*. Авторы разбирают каждый пример с технической изнанки, давая читателю редкий по емкости и четкости анализ инструментария кибервойн — от примитивных DDoS-атак и типовых *логических бомб* до сверхсложных червей, выводящих из строя промышленное оборудование, и программ, позволяющих *ослеплять* современные системы ПВО.

Оставляя ответ на усмотрение читателя, Кларк озадачивает его очередным вопросом — если кибервойна реальна, кто же ее ведет? Ничтоже сумняшеся, объявляя РФ основным *дирижером* и организатором атак на Грузию и Эстонию, авторы все же признают и подробно рассматривают *проблему атрибуции* — одно из ключевых препятствий к предотвращению кибервойн. Несмотря на это, в фокусе внимания оказываются не анонимные хакерские группировки или кибертеррористы — последним в книге почти не отводится места, что вообще симптоматично с учетом послужного списка Кларка, — а государственные или квазигосударственные структуры.

В главе *Кибервоины* дается прекрасный обзор того, как в американских госструктурах на организационном уровне оформлялась повестка военно-стратегической кибербезопасности. В 2009 г. этот процесс увенчался созданием Киберкомандования, но отнюдь не закончился. Кларк дарит читателю отличную возможность проникнуть в лабиринты межведомственной борьбы за контроль над военной киберповесткой в американских спецслужбах и армии. Где еще можно из первых рук узнать подноготную затяжного *перетягивания каната* между киберподразделениями ВМС, ВМФ и Сухопутных сил США? Вникнуть в суть дискуссии о том, на каком структурном уровне должна была быть обособлена кибероборона — от 10-го флота в составе ВМС (или субструктуры ВВС) до нового *вида* войск — и насколько причудливым и гибким компромиссом в этом смысле стало Киберкомандование в его нынешнем виде?

Вслед за США анализируется КНР с многоуровневой системой всевозможных сообществ, ведущих борьбу в киберпространстве в интересах Поднебесной и в различной степени связанных с государством. На вершине этой пирамиды находятся секретные штатные киберподразделения НОАК, в основании — обычные китайские граждане, которые нередко выражают свои патриотические чувства, участвуя в DDoS-атаках на ресурсы государств или компаний, навлекших на себя гнев Пекина. В середине же этой сложной иерархии — масса университетов, исследовательских центров и иных окологосударственных учреждений, полурегулярных ассоциаций и группировок сетевых активистов и патриотичных *кибервоинов*, которых трудно сосчитать. На фоне подробного анализа структур кибероборонны (и, в не меньшей степени, кибернападения) немного теряется Россия, в отношении которой познания авторов заканчиваются на Федеральном агентстве правительственной связи и информации при Президенте РФ (ФАПСИ), упраздненном в 2003 г., а также расплывчатом упоминании Главного разведывательного управления и Службы внешней разведки. Что ж, для российских спецслужб столь скудные познания о них американских коллег могут считаться и поводом для гордости.

Глава 3, *Поле битвы*, посвящена рассмотрению того, где, в каких сетях ведется или, скорее всего, будет вестись кибервойна и какие свойства сетей делают кибервойну не только реальной, но и весьма вероятной уже сегодня. Авторы рассматривают особенности и уязвимость интернета, связывающего воедино изолированные островки киберпространства. Уязвимость Сети делает возможным перехват информации, ее изменение, удаление, нарушение работы глобальной системы доменных имен (DNS) и, в конечном счете, разрушение целостности киберпространства. Все это позволяет авторам говорить о том, что в кибервойне интернет может выступать как основным пространством и *каналом* для агрессивных действий, так и их конечной *целью*. При этом в мире развивается процесс усиления зависимости промышленных, военных и иных критических технологий от информационных систем. Компьютеры и сети необходимы для функционирования современной финансовой системы, транспортной и энергетической логистики всех видов, энергогенерирующих и энергораспределительных систем и, конечно, передовых военных разработок.

По большинству параметров США являются наиболее зависимой от кибертехнологий нацией в мире, вплоть до того, что оптимизация промышленных процессов требует подключения автоматизированной системы управления технологическим процессом (АСУ ТП) не просто к локальным сетям, а к интернету, а соединения войск, унаследовавших парадигму *сетецентричности* от администрации Буша-младшего, при нарушениях сетевых коммуникаций теряют боеспособность. Особым *пунктом,* на который авторы раз за разом делают упор, является уязви-

мость энергосетей и генерирующих мощностей, в основном находящихся в частной собственности. Кларку явно неуютно от того, что возможности федерального регулирования, которое повысило бы стандарты кибербезопасности на объектах энергосистемы США и обязало операторов изолировать АСУ ТП от интернета (или хотя бы должным образом шифровать управление энергомощностями), ограничены и наталкиваются на неизменное сопротивление лоббистских группировок. Между тем, именно информационные системы энергосетей и генераторов на электростанциях стали самым лакомым куском для китайских и прочих хакеров, которые уже напичкали их *потайными входами* и *логическими бомбами*, отследить и обезвредить которые полностью невозможно.

Это обусловливает несопоставимую с потенциальными противниками уязвимость США в случае кибервойны. Одна из главных задач, которую ставит перед собой Кларк — донести до Белого дома, Пентагона, а заодно и массовой аудитории тезис о том, что высокий уровень развития ИКТ может стать для США *ахиллесовой пятой* в случае конфликта. При этом превосходящий потенциал *кибернападения*, которое грозит превратиться в *доктринальный фетиш* в стенах Пентагона, не компенсирует уязвимость и зачастую нивелируется меньшей зависимостью потенциальных противников от киберинфраструктуры. Любопытной, хотя и небесспорной иллюстрацией парадоксов потенциала государств в киберпространстве служит таблица, приводимая Кларком в главе 5, *На пути к стратегии обороны*. Для того чтобы сопоставить потенциал США и их вероятных противников в кибервойне (КНР, РФ, Ирана и КНДР), вводятся три равновесных показателя — потенциалы кибернападения и кибероборонs, а также степень зависимости национальной инфраструктуры и экономики от кибертехнологий. В итоге США уступают всем вероятным оппонентам, а высший балл получает... КНДР, несмотря на довольно слабый наступательный киберпотенциал. Такая оценка парадоксальна, но справедлива в том смысле, что разрушение примитивной киберинфраструктуры КНДР, во-первых, никак не скажется на экономике и военной мощи страны, а во-вторых, не компенсирует тот ущерб, которые вражеские *кибервоины* теоретически могут нанести США.

А на описание последствий кибервойны для США Кларк с коллегой не скупятся, рисуя поистине апокалиптическую картину: взрывы на химических заводах и токсичные облака над мегаполисами, пожары на нефтехранилищах и трубопроводах, транспортный коллапс на дорогах и в аэропортах. Нация оказывается буквально парализована без электричества, управления, защиты и информации о том, что происходит. Пожалуй, Кларка можно упрекнуть в алармизме и преувеличении рисков такого сценария. В нем все же говорит чиновник, чье видение информационных технологий много лет формировалось сквозь призму исходящих от них угроз. Однако в кейсе о киберконфликте США и КНР в недалеком будущем (сюжет, уже ставший *sine qua non* в публикациях американских стратегов на тему кибервойн), авторы рисуют довольно сдержанный сценарий. Стороны обмениваются взломами секретных военных сетей, локальными *блэкаутами* в нескольких регионах, выводом из строя спутниковых коммуникаций и транспортной логистики. Человеческие жертвы отсутствуют или минимальны. И хотя США терпят поражение, для мира история скрыта за завесой дипломатических маневров, позволяющих Вашингтону худо-бедно сохранить лицо.

Чего же хотят авторы от нынешних хозяев Белого дома и адресован ли их труд только американскому политическому истеблишменту? Нет, не только — Ричард Кларк рискует углубляться в тему международно-правового регулирования поведения государств в киберпространстве, и это, пожалуй, наиболее ценная и актуальная для российского читателя часть *Кибервойны*. Если бы книга состояла лишь из главы *Кибермир*, полностью посвященной проблемам создания международного режима предотвращения кибервойн и регулирования применения кибероружия, она все равно стала бы одной из выдающихся публикаций на тему кибербезопасности за последние годы. В начале главы Кларк невзначай признается: именно он от лица США *зарубил* первые инициативы РФ по созданию международного режима предотвращения информационных войн, озвученные на площадке ООН еще в 1998 г., и продолжал блокировать их до ухода с госслужбы. Впрочем, заложенный

им курс был сохранен и после 2003 г. и до последнего времени поддерживался без сколько-нибудь существенных изменений.

В чем же дело? Кларк не стесняется называть российские инициативы пропагандой, лишенной реального содержания и направленной скорее на саботаж международного взаимодействия. Издание, правда, вышло до того, как осенью 2011 г. РФ презентовала концепцию Конвенции об обеспечении международной информационной безопасности, а четыре государства — члена ШОС, включая РФ и КНР, направили Генсеку ООН письмо с проектом Правил поведения в области международной информационной безопасности. Однако можно смело утверждать, что тональность г-на Кларка вряд ли существенно изменилась бы. Конечно, утверждения о пропагандистском характере российских предложений, как минимум, спорны и невольно вызывают желание обвинить автора в тенденциозности, тем более что не подкрепляются сколько-нибудь серьезными аргументами. По размышлении над прочитанным кажется, что проблема вовсе не в этом и на самом деле для США неприемлем *всеобъемлющий подход*, заложенный в основу инициатив Москвы. По мнению авторов *Кибервойны*, какое-либо комплексное соглашение ведущих мировых держав об отказе от ведения кибервойн — не говоря уже про кибершпионаж, а также от разработки кибероружия попросту невозможно, так как не подлежит эффективному контролю и не обеспечивается достаточными стимулами. Исходя из такой логики предложения и меры, составляющие суть российских инициатив, действительно неприемлемы для США.

Насколько Кларк прав *в этой части* — вопрос для отдельного большого исследования, но некоторые меры из числа названных в книге заслуживают внимания. В том числе, идея начать строительство международного режима кибербезопасности с точечных соглашений об ограничении либо запрете инициированных государствами кибератак на отдельные системы и объекты. Например, такие как информационная инфраструктура глобальной финансовой системы, от которой равно зависимы США, КНР, Россия и даже Иран. Сюда же напрашивается еще один перечень таких объектов, о котором Кларк лукаво умалчивает, несмотря на наличие в переиздании книги подробного комментария о черве *Stuxnet*. Почему бы не включить в такое соглашение инфраструктуру объектов, связанных с оружием массового уничтожения (ОМУ), и особо опасных *чувствительных* промышленных объектов, таких как АЭС, химические заводы и т. п.? Среди прочих идей авторов — соглашение о неприменении кибервооружений первыми даже в случае конфликта с использованием обычных вооружений, запрет атак на гражданскую инфраструктуру, включая в первую очередь энергосети.

Ключевая идея подхода, изложенного на страницах книги, — не пытаться добиться полного запрета кибервойн *с нуля*, из сегодняшнего состояния, близкого к анархии, а пошагово *взращивать* режим безопасности киберпространства, фиксируя и понемногу расширяя минимальные точки совпадения интересов основных игроков на международной арене. Кларк не случайно так часто и упорно ссылается на опыт режима контроля над ядерными вооружениями, который в основном сложился за время холодной войны. Тот режим формировался более 30 лет, и его развитие не завершилось до сих пор, как показывают яростные дискуссии вокруг глобальной ПРО США и ядерной программы Ирана. И начинался он с малого — например, с временного соглашения между СССР и США об ограничении стратегических наступательных вооружений (ОСВ-1), договоров о запрещении испытаний ядерного оружия в отдельных средах. Потребовались десятилетия с момента создания атомной бомбы и острейший Карибский кризис, прежде чем стороны перешли к вопросам *сокращения* ядерных арсеналов и перестали рассматривать нанесение массированных ядерных ударов по противнику в качестве реально применимого внешнеполитического инструмента. В эпоху кибертехнологий время течет несравнимо быстрее, однако база для режима безопасности киберпространства все же должна вызреть, вырасти из локальных соглашений и ограниченного консенсуса по отдельным вопросам.

По крайней мере, так считают авторы *Кибервойны*. Правы они или нет, судить читателю, в том числе и российскому. Но для этого труд Ричарда Кларка и Роберта Кнейка должен обязательно попасть на наши книжные полки — он того заслуживает.

David E. Sanger. Confront and conceal: Obama's Secret Wars and Surprising Use of American Power. N. Y.: Crown Publishers, 2012. 498 p.

Кинга Дэвида Сэнгера *Противостоять и скрывать: тайные войны Обамы и неожиданное использование американской силы* была опубликована в США в начале июня 2012 г. и сразу стала бестселлером. Сейчас ее спешно переводят на другие языки. То, что книга будет пользоваться большой популярностью в США и за их пределами, было понятно еще до ее выхода — сенсацию произвела даже краткая выдержка из работы Сэнгера, напечатанная газетой *The New York Times* за неделю до официальной публикации. Отчасти это объясняется личностью автора — 52-летний Сэнгер — один из самых известных журналистов *The New York Times*, его статьи дважды были отмечены Пулитцеровской премией. За плечами у Сэнгера много лет работы в пуле президента США в качестве аккредитованного корреспондента, его часто приглашают на телевидение как *эксперта по Белому дому*. Иными словами, произведенному книгой фурору во многом способствовал авторитет ее автора.

Содержание книги в целом можно передать одной фразой: компьютерный вирус *Stuxnet*, существенно замедливший иранскую ядерную программу, придумали в Белом доме. О том, что *Stuxnet* разработали специалисты из США и Израиля, пресса писала и до Сэнгера. Но ранее никто не рассказывал, как именно это происходило, кто всем руководил и почему в итоге все пошло наперекосяк. Сэнгер же приводит отчет о секретной правительственной программе по созданию *Stuxnet* чуть ли не по часам. Правда, в его работе все же присутствует один минус, не позволяющий окончательно расставить *точки над i* — практически все источники в книге Сэнгера анонимны. Впрочем, это вполне объяснимо, ведь в числе источников и чиновники администрации президента, и сотрудники Госдепа и Пентагона, и высокопоставленные офицеры американских спецслужб. Учитывая весьма чувствительный характер сообщаемой информации, едва ли кто-то из них рискнул бы раскрыть свое имя для публикации. Впрочем, этот факт не умаляет ценности труда Сэнгера для всех, кто хоть мало-мальски интересуется кибербезопасностью, политикой Вашингтона и отношениями США с Израилем и Ираном. Автор рассказывает все настолько подробно и с таким количеством нюансов, которые могут быть известны только инсайдерам, что ему действительно хочется верить.

Книга разбита на несколько частей. Первую можно, в принципе, пропустить. Автор, видимо, стремясь расширить свою аудиторию за счет неспециалистов в международной политике, начинает повествование *от царя Гороха* — с рассказа про действия США в Афганистане и Пакистане. Самое интересное начинается во второй главе, повествующей о том, как во время своего второго президентского срока Джордж Буш-младший санкционировал запуск секретной программы по созданию

передового кибероружия, а позднее завещал ее своему *преемнику* — Бараку Обаме. Соответствующую операцию под кодовым названием *Олимпийские игры* еще в 2006 г. разработало ЦРУ. Тогдашнему американскому президенту ее представил глава Стратегического командования вооруженных сил США генерал Джеймс Картрайт. По словам Сэнгера, тогда *ястребы* вроде вице-президента Дика Чейни активно убеждали Джорджа Буш-младшего в необходимости нанесения военного удара по иранским ядерным объектам. Картрайт и специалисты из ЦРУ предложили *щадящий* вариант — создание мощного компьютерного вируса, который смог бы вывести из строя центрифуги на иранском обогатительном комбинате в Натанзе. Американский президент изначально скептически отнесся к этой идее, но тем не менее выделил средства на развитие программы.

На создание вируса ушло несколько месяцев, еще столько же времени понадобилось для тестирования его потенциала. *Stuxnet* удалось внедрить во внутренние информационные сети завода в Натанзе в 2008 г. Первые сбои в работе систем комбината были не слишком серьезными, однако в Вашингтон стали поступать сведения о панике среди иранцев. Самым гениальным свойством вируса, по словам разработчиков, была его способность *убеждать* автоматизированные системы управления комбината в том, что все центрифуги работают исправно, в то время как они одна за другой выходили из строя.

Барак Обама, как следует из книги Сэнгера, прислушался к совету бывшего президента и не только не стал сворачивать программу, но уже в течение первых нескольких месяцев после занятия поста президента в 2009 г. распорядился расширить ее. Атаки на Натанз активизировались. Однако летом 2010 г. вирус *вырвался на свободу*. Предположительно, он *перескочил* на ноутбук одного из иранских инженеров, а потом попал в глобальную сеть, где и был обнаружен программистами одной из компьютерных лабораторий, прозвавшими его *Stuxnet*. Источники Сэнгера утверждают, что *Олимпийские игры* замедлили иранскую ядерную программу на полтора-два года.

Нельзя сказать, что публикация *Противостоять и скрывать* обрадовала всю читательскую аудиторию. Сразу после выхода книги ей активно заинтересовался Конгресс США: инициативная группа конгрессменов-республиканцев потребовала расследовать факт утечки данных, содержащихся в работе Сэнгера. По их мнению, разглашение информации о кибероперациях США наносит ущерб национальной безопасности, так как другие страны могут пойти тем же путем. Результаты расследования, инициированного Конгрессом, могут быть обнародованы уже до конца 2012 г.

Однако самого Сэнгера подобная реакция, судя по всему, не сильно расстроила: своими настойчивыми требованиями конгрессмены фактически подтверждают, что все, о чем пишет автор, — правда. Российскому читателю стоит ознакомиться с этой правдой *из первых рук* — ведь события, связанные со *Stuxnet*, на деле куда важнее многих раскрученных сенсаций вроде откровений американских спецназовцев об операции по устранению Бен Ладена.

Елена Черненко

Franklin D. Kramer, Stuart H. Starr, Larry Wentz. Cyberpower and National Security. Washington, D.C: Potomac Books, 2009. 642 p.

Первое, что бросается в глаза, после того как берешь книгу в руки, — это ее название: *Киберсила и национальная безопасность*. В нем нет порядком набивших оскомину слов в книгах подобного жанра — киберугрозы, кибертерроризм, информационные операции и т. д. А уже после прочтения понимаешь, что на протяжении более чем 600 страниц практически не встречается сам термин *кибербезопасность*. Уже исходя из этого можно утверждать, что имеешь дело не с очеред-

ной научно-фантастической повестью или наукообразной беллетристикой на тему кибертехнологий, а с солидным трудом, чьи авторы всерьез претендуют на теоретическое осмысление того, что такое киберпространство и как оно может быть вписано в общую стратегию национальной безопасности США.

Стоит упомянуть, что книга была написана в рамках проекта Центра технологий и политики в области национальной безопасности Национального университета обороны США. Над проектом работал очень широкий круг исследователей и экспертов в области киберпространства, а также военных. Практическая каждая глава книги написана разными авторами или коллективами авторов, которые зачастую придерживаются разных подходов к проблеме или используют несовпадающую терминологию. Однако, несмотря на это, редакторам удалось очень эффективно структурировать содержание труда, разбив его на шесть базовых частей: *Основы и обзор проблематики, Киберпространство, Киберсила: военное использование и сдерживание, Киберсила: информация, Киберсила: стратегические проблемы и Институциональные факторы*.

В первом разделе дается общий обзор проблем в сфере киберпространства; авторы пытаются выработать целостный подход для их решения. Прежде всего выделяются основные политические факторы, которые будут в дальнейшем влиять на выработку национальной стратегии безопасности в киберпространстве. Условно говоря, они делятся на внутренние (человеческий капитал, институты, принципы управления) и внешние (сетевые операции, проблемы сдерживания, атаки против компьютерных сетей). С учетом трансграничности киберпространства для обеспечения благоприятного развития этих факторов государство должно активно развивать международное сотрудничество через взаимодействие с военными союзниками, поддержание высокого уровня международного влияния с помощью публичной дипломатии, а также усиление международных структур управления киберпространством. В последующих главах раздела авторы попытались сформировать целостную теорию киберпространства и *киберсилы*, хотя и без особых успехов. Очень похоже, что даже передовым экспертам пока еще недостает ни теоретических междисциплинарных знаний, ни практического опыта для реализации столь амбициозных задач.

В разделе *Киберпространство* упор сделан на рассмотрении структурных элементов киберпространства и на том, какие изменения оно может претерпеть в среднесрочной перспективе. Достаточно подробно рассматривается вопрос взаимодействия различных уровней киберпространства — инфраструктурного, логического, информационного и социального. Большое внимание также уделяется тому, как происходит взаимодействие киберпространства и объектов инфраструктуры и какие уязвимости для последней возникают в результате. Для минимизации угроз в первую очередь предлагается сконцентрироваться на регулировании и эффективном распределении полномочий как между местными и федеральными властями, так и между государством и бизнесом.

Вместе с тем за прошедшее время с момента публикации *Киберсилы* возникла необходимость в выработке международных норм по недопущению атак, например, против элементов гражданской инфраструктуры, таких как школы, больницы и т. п. В отношении эволюции развития киберпространства, наибольшее внимание уделено краткосрочным трендам — таким, к примеру, как развитие *интернета вещей* [the internet of things]. В то же время из поля внимания авторов почти ускользнуло рассмотрение средне- и долгосрочных трендов развития киберпространства. Из числа последних в книге освещаются лишь биотехнологии и перспективы их конвергенции с информационно-коммуникационными технологиями (ИКТ). Почти не затрагивается возможное влияние нано- или квантовых технологий на уровень физической инфраструктуры, равно как и их опосредованное влияние на остальные уровни киберпространства.

Последующие три раздела посвящены тому, как киберпространство может быть использовано в качестве нового *поля боя* и как внутри него формируются угрозы

национальной безопасности. В традиционной для американцев манере информационное пространство рассматривается в качестве нового поля ведения военных действий наравне с землей, морем, воздухом и космосом. В числе основных факторов, способствующих успешному использованию любого поля боя, выделяются технологическое превосходство, масштаб и скорость действия, контроль ключевых позиций и национальная мобилизация. По мнению авторов, все эти факторы в равной мере присущи и киберпространству. К примеру, использование компьютерных технологий при сетевых операциях позволяет повысить эффективность боевых действий во всех остальных *средах*.

Примечательно, что авторы многостраничного труда в отдельный раздел выносят институциональные аспекты управления киберпространством, такие как глобальное управление интернетом и международно-правовое регулирование киберпространства. Более того, обозначенный круг вопросов позиционируется как отдельное направление национальной политики, которое должно развиваться *параллельно* с национальной безопасностью, но не обязательно в ее рамках.

Впрочем, труд американских *кибертеоретиков* все же имеет достаточно серьезный недостаток — в глаза бросается отсутствие заключительной главы, которая емко резюмировала бы проделанную работу. С другой стороны, такой раздел мог оказаться излишним: достаточно открыть перечень стратегических документов США в области киберпространства, принятых после публикации этой книги, чтобы воочию увидеть ее заключительные главы. Поэтому книга будет интересна и полезна для всех, включая любителей узнать что-то новое, начинающих исследователей в области киберпространства и *киберсилы* (для которых она может стать настольной книгой), а также для лиц, принимающих решения.

Максим Симоненко

P. W. Singer. Wired for War. The Robotics Revolution and Conflict in the 21st Century. London: Penguin Books, 2010. 499 p.

В России пока еще не научились писать *non-fiction* и научную литературу в близком широким кругам стиле. В Америке бестселлер газеты *The New York Times* может носить подзаголовок *Революция в робототехнике и конфликты XXI века* и повествовать об изменении характера войны в будущем, в то же время на обложку будет вынесен комментарий «начисто вынесла мне мозг... крутая книжка». При этом сам автор на вопрос о том, почему он потратил четыре года на освещение темы, ничтоже сумняшеся отвечает: «Потому что роботы чертовски крутые». При этом обвинить в маргинальности Питера Сингера, автора книги и директора проекта *Оборонная инициатива для XXI века* Брукингского института, успевшего поработать в Гарварде, Пентагоне и Международном институте мира, язык не поворачивается. Скорее перед нами плод типичного для США скрещивания научной и популярной литературы: так и книгу продавать проще, да и вообще, каким еще языком писать про роботов?

Как бы то ни было, *Wired for War* на сегодняшний день остается одним из самых подробных и интересных исследований на тему того, как робототехника меняет привычный нам подход к военным действиям, а разбросанные по тексту небрежные упоминания о том, что в 2008 г. Министерство обороны США имело на вооружении 5331 беспилотник, или краткое описание тактики использования малых беспилотников типа *Raven* в Ираке, заставляют руку потянуться за карандашом или, как минимум, *завязать мысленный узелок*.

Сангер строит беседу с читателем в беспроигрышном ключе. Повествование начинается с того, что вынесенная в заголовок книги революция фактически состоялась — роботы уже несут военную службу на земле, в воде и воздухе, на заморских театрах военных действий и в метрополии, и только генералы, как обычно,

готовятся к прошедшей войне. Автор так полно описывает последние технические решения в военной сфере, что книжка очень полезна, хотя бы для того, чтобы разобраться, что из того, что показывают в научно-фантастических фильмах, уже реально существует. Похоже, практически все.

Вопросы, возникающие при описании огромного арсенала оружия (излучатели звуковых волн, *клееметы*, микроволновые и радиоволновые пушки, метатели плазмы), дополненного различными автономными платформами, следующие: как получилось, что Афганистан и Ирак все еще не зачищены от боевиков и почему основную тяжесть военных действий по-прежнему несут на себе люди, вооруженные старыми добрыми *M-16*? Прямого ответа Сангер не дает, но, видимо, подразумевает, что это вопрос 10–20 лет, и, чтобы показать динамику процесса, проводит читателю увлекательную обзорную экскурсию, описывая истоки робототехники от Аристотеля и механических игрушек Жака Вокансона до современности и прогнозирования будущего.

Получается захватывающая и эпическая картина, в которой находится место историям о том, как связана с беспилотниками Мэрилин Монро, и почему слово *bugs* стало обозначать ошибки в программном коде. И если с рядом положений автора — в частности, слишком вольной трактовкой понятия *сингулярность*, — можно поспорить, то фактологическая сторона проработана блестяще. Складывается впечатление, что автор лично обошел всех сколько-нибудь значимых игроков на описываемом поле.

Учитывая, что большинство подобных компаний расположено в США, книга стала отчасти напоминать *yellow pages* американской робототехники, а название государственного агентства DARPA, инвестирующего в разработки, появляется в тексте не реже, чем слово *робот*. Что, конечно, ничуть не умаляет ценности агентства.

Вообще от прочтения книги остается впечатление, что весь остальной мир отстал от Соединенных Штатов как минимум на десятилетие. Американские ученые с небольшой помощью британских, японских и израильских коллег (может именно это и объясняет союзнические отношения между государствами) с увлечением и задором создают даже не столько оружие, сколько новые технологии, принципы и концепции. Чем-то подобным занимались герои книги *Понедельник начинается в субботу* — с той лишь разницей, что в нашем случае главным распорядителем выступает не идеальный советский НИИ, а вполне реальное Министерство обороны США. Если российская *оборонка* ничем подобным не занимается, то отрыв выглядит катастрофическим. Ну а если занимается, нужно срочно садиться и готовить собственную книгу.

Андрей Баклицкий

Joel Brenner. America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. N. Y.: The Penguin Press. 2011. 320 p.

Вышедшая в 2011 г. книга Джоэла Бреннера, одной из знаковых фигур американской контрразведки прошлого десятилетия, примечательна прежде всего личностью автора. Бреннер известен как глава контрразведки в Управлении директора Национальной разведки США с 2006 по 2009 г., при администрациях Буша и Обамы. До этого послужной список г-на Бреннера включал в себя должности старшего советника в Агентстве национальной безопасности США, ответственного за вопросы безопасности информационных сетей и генерального инспектора АНБ в первой половине *нулевой* декады. Годами на этом человеке замыкались нити организационной работы и теоретического прогресса американской контрразведки в киберпространстве. Уже по этой причине его мнение нельзя считать сколь

угодно квалифицированным *внешним* экспертным анализом — это взгляд на проблему *изнутри*.

Именно так и формулирует автор свой подход в заглавии труда, которое с некоторой погрешностью переводится на русский как *Уязвимая Америка: взгляд изнутри матрицы новых угроз цифрового шпионажа, преступности и войны*. В названии кроется вторая особенность, которая делает книгу рекомендованной к прочтению экспертам в сфере информационной безопасности — автор не ограничивает рассматриваемый круг вопросов собственно электронной разведкой и шпионажем, предлагая анализ киберугроз по всему их спектру. И, удивительным или ожидаемым образом, на первом плане оказываются угрозы военно-стратегического характера, исходящие от национальных государств — России и Китая. Точнее, от Китая. Едва ли не половина книги Бреннера так или иначе отсылает читателя к деятельности КНР в киберпространстве, что само по себе много говорит о том, какое внимание уделяет ей американский разведывательный истеблишмент.

Живописание китайской угрозы вообще выглядит наиболее яркой, информативной и убедительной частью книги. Конечно, Бреннер не забывает рассказать о структурной чехарде и смене концепций, сопровождающих становление американской контрразведки в киберпространстве, подходах к частному сектору, проблеме киберпреступности и т. д. Но настоящими *бриллиантами* на страницах *Уязвимой Америки* выглядят главы, в которых автор, жонглируя цифрами, датами и именами, описывает, что, как и в каких размерах делают китайцы с сетями США и какие последствия это может иметь для национальной безопасности Америки. Кража данных о новейшей системе компьютерного управления корабельным огнем Aegis, лежащей в основе морского компонента ПРО США, похищение технической информации об истребителе пятого поколения *F-35* и двигателях американских тихоходных АПЛ и многие другие инциденты рассматриваются Бреннером с особым вниманием. Перечень их способен напугать даже тех читателей, которые не очень переживают за национальную безопасность наших западных партнеров.

Не останавливаясь на размахе китайского (а с ним менее масштабного, но более изощренного российского) кибершпионажа, автор повествует об угрозах *кибер-саботажа*, которые обусловливает повсеместная уязвимость американских сетей. Нужно отдельно сказать о том, как оценивается степень этой уязвимости — из книги Бреннера становится ясно, что в военных и разведывательных кругах США утверждается принцип действовать и принимать решения исходя из того, что служебные сети — включая секретные — *повсеместно* взломаны. В случае Пентагона, например, речь идет не только о NIPRNET — сети, содержащей несекретные данные для служебного пользования, но и о SIPRNET и JWICS — секретной и, соответственно, сверхсекретной сетях оборонного ведомства. И это заставляет осознать масштаб проблемы. Попробуйте представить себе, что должно произойти, чтобы такой принцип утвердился в Минобороны РФ или в ГРУ. Однако разрушительный потенциал *киберсаботажа* основан не на уязвимостях сетей военных и спецслужб, а на слабой защите критической промышленной инфраструктуры США, которая не подпадает под жесткое государственное регулирование, находясь преимущественно в частной собственности.

По мнению Бреннера, главный дьявол таится именно здесь. Одним из тезисов, идущих через книгу красной нитью, является уязвимость электрических сетей США. В частности, речь идет об отсутствии должной защиты автоматизированных систем управления технологическим процессом (АСУ ТП), контролирующих работу основных генераторов на электростанциях. Бреннер, конечно же, ссылается и на известный специалистам эксперимент *AURORA*, в ходе которого в 2007 г. команде специалистов из Национальной лаборатории Айдахо удалось взломать АСУ ТП промышленного электрогенератора и добиться физического разрушения его турбины, используя исключительно программный код. Бреннер не устает предупреждать и о том, что информационные системы электрических сетей и энергогенерирующих систем США уже *напичканы* китайскими *потайными ходами* и *логи-*

ческими бомбами, которые в любой нужный момент могут быть задействованы *кибервоинами* КНР.

Все угрозы национальной безопасности США из киберпространства сводятся Бреннером воедино в блестящем кейсе — пожалуй, самом захватывающем разделе книги. Глава *Июнь 2017* повествует об эскалации дипломатического кризиса между США и КНР по поводу Тайваня в ближайшем будущем. Эскалация не ведет к открытому конфликту, но перерастает в китайско-американскую кибервойну, в которой США терпят оглушительное поражение. Сценарий событий прописан крайне убедительно, в немалой степени потому, что Бреннер воздерживается от апокалипсических картин, которыми изобилует схожий кейс в вышедшей за год до *Уязвимой Америки* книге Ричарда Кларка *Кибервойна*. Действия китайских хакеров не ведут к взрывам химических заводов, крушению поездов метро, массовому падению гражданских авиалайнеров — достаточно убедительной демонстрации возможностей.

Покажите, что вы можете погрузить во тьму базы разведслужб и американского Киберкомандования, стереть данные в секретных сетях Пентагона, заставить смертоносные *Рапторы* падать в море подбитыми птицами, активировав *закладки* в их бортовых системах. Дайте противнику понять, что он толком не знает ни вашего потенциала, ни собственных уязвимостей. И несокрушимые американские авианосцы сами развернутся и уплывут к родным берегам, а хозяин Белого дома пойдет на попятную в, казалось бы, принципиальных вопросах. А мир так ничего и не узнает... или сделает вид. Бреннер отнюдь не стремится запугать читателя, он описывает то, что пугает и тревожит его самого и, по-видимому, многих военных и сотрудников разведслужб США.

Ко всему прочему, автор считает нужным дать читателю глубокий, въедливый анализ того, как зародилась, эволюционировала и пришла к нынешнему виду китайская стратегия поведения в киберпространстве. Эта ретроспектива очень полезна российской аудитории, так как проливает свет на вехи стратегической мысли нашего восточного соседа и стратегического партнера, которые обычно остаются на периферии внимания. Часто ли в русскоязычной дискуссии заходит речь о революционном значении *Бури в пустыне* 1991 г. для военной стратегии КНР, которая в итоге отринула идею войны массовыми армиями и судорожно начавшей поиски новой доктрины, способной нивелировать колоссальное на тот момент технологическое превосходство США? Многие ли понимают значение брошюры, написанной в 1999 г. двумя малопримечательными китайскими полковниками и переведенной на английский под заголовком *Неограниченная война: китайский план по уничтожению Америки*? Пытается ли экспертное сообщество понять, насколько уникальным *объектом* такой доктрины являются США, и может ли она при первой потребности быть переориентирована на Россию? И не пора ли от традиционных страхов китайского военного вторжения в Сибирь переходить к анализу более актуальных рисков, таких как попадание РФ под *молот* китайского кибершионажа и киберсаботажа? Ведь в киберпространстве у Поднебесной нет стратегических партнеров и *запретных целей*, равно как и однозначных противников, отношения с которыми должны развиваться исключительно в плоскости конфликта.

Конечно, господин Бреннер отнюдь не стремится выходить за рамки рассмотрения национальных интересов США в киберпространстве и доносить все эти вопросы до российской аудитории. Достаточно однобоко характеризуя РФ как угрозу № 2 безопасности Америки в киберпространстве, бывший глава контрразведки не стесняется выдвигать забавную и неуклюжую версию *российского* авторства червя *Stuxnet*, выведшего из строя центрифуги в иранском Натанзе в 2010 г. В самом деле, не писать же ему, что да, действительно, *Stuxnet* создавался американскими и израильскими специалистами под контролем спецслужб и явно не без участия его ведомства. Любопытный момент: характеризуя потенциал и приводя примеры враждебных кибероперацій РФ, КНР и других стран, Бреннер не считает нужным вдаваться в анализ перспектив международного сотрудничества по обеспечению безопасности киберпространства. Приземленный взгляд контрразвед-

чика отмечает анархичное состояние международного сообщества и отсутствие твердых правил поведения в киберпространстве, которое позволяет даже ближайшим союзникам США не гнушаться кибершпионажем и другими недружественными по отношению к Вашингтону операциями.

Но задачи вырабатывать какие-либо правила и рамки для международной повестки у Бреннера нет — его рекомендации носят весьма практический характер и адресованы госструктурам и частному сектору США. В части рекомендаций федеральным агентствам нет сногсшибательных откровений, хотя присутствуют полезные идеи: обязать шестерку ключевых провайдеров в США уведомлять пользователей о том, что их компьютеры используются в качестве части ботнетов, нормативно ограничить возможности подключения к Сети АСУ ТП объектов электроэнергетики, находящихся в частной собственности, снять антитрастовые ограничения на деятельность американских компаний в области разработки систем и технологий защиты от киберинцидентов и т. д. Рекомендации частному сектору выглядят более стандартно и выхолощено, может быть по причине того, что здесь Бреннер ступает на менее знакомую ему почву.

В своей книге Бреннер не забывает рассказать, как развитие информационных технологий отразилось на принципах, облике и самой сути разведки и контрразведки. *Жизнь в стеклянном доме,* как характеризует автор сегодняшнее состояние разведки, трансформирует привычную агентурную работу, способы осуществления операций и контроопераций. Она дарит контрразведке огромные возможности (сбор информации через социальные сети, вебкамеры, спутниковые и геолокационные системы), но в то же время ставит перед ней беспрецедентные вызовы (сохранение секретов в тотально проницаемой среде). Заглядывая в будущее, Бреннер делится с читателем парадоксальным, но в то же время закономерным выводом: максимум через пару десятилетий все мы будем жить в мире, где сокрытие информации станет невозможным. Всех нас ждет жизнь в *стеклянном доме,* и подготовиться к ней необходимо заранее, чтобы в один прекрасный день *скелеты в шкафу* не принесли каждому из нас большие неприятности. Особенно если в числе таких *скелетов* — уязвимости национальной критической инфраструктуры, стратегические военные технологии, потоки финансовых данных и передовые научно-технологические разработки частного сектора стоимостью многие миллиарды долларов.

В общем и целом, у Джоэла Бреннера гораздо лучше получилось осветить спектр проблем, чем предложить решения. Однако *Уязвимая Америка* все же заслуживает того, чтобы попасть на книжные полки экспертов в области информационной безопасности — ведь в *стеклянном доме* уязвима не только Америка, но и ее соседи, включая старых *заклятых друзей* по эту сторону Атлантики.

Олег Демидов

ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕГОДНЯ: АЛОГИЗМЫ РАЗВИТИЯ

Главному редактору:

Только ленивый, рассуждая о новых угрозах в контексте постмодерна, не говорит об информационной безопасности. Но лишь немногие, за исключением разве что глубоких профильных специалистов, могут ответить на вопрос, что же такое информационная безопасность сегодня.

В преамбуле к свежему официальному документу уровня ООН одной из стран *Большой семерки* сказано: «Киберпространство играет ключевую роль в поддержании инновационной всепланетной экономики и обеспечения связи между обществами; оно позволяет предпринимательству свободно заниматься инновациями, снижением себестоимости и поиском доступа к новым рынкам. Логичные, последовательные и предсказуемые взаимодействия в киберпространстве помогут поддержать всепланетную инновационную цифровую экономику, энергичное, многообразное и подключенное всепланетное общество, укрепить международный мир и безопасность»[1]. Гораздо проще сказано в соглашении стран — членов Шанхайской организации сотрудничества (ШОС) о сотрудничестве в области информационной безопасности: «Информационная безопасность — состояние защищенности личности общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве»[2]. При этом второе определение, несмотря на кажущуюся простоту, ближе подходит к сути вопроса и в меньшей степени нуждается в пояснениях.

В начале 1990-х гг., когда термин *информационная безопасность*[3] только начал появляться в политологических работах, обозначаемая им сфера отношений понималась как антипод *информационной войны*. Отсюда и берет начало та несостыковка сути современного понятия информационной безопасности и того формального наполнения, которое иногда в это понятие вкладывается *по инерции*. Причем сама информационная война тогда определялась не иначе как в стилистике межгосударственного силового противоборства. Не исключалось, правда, что участниками конфликта могут быть и негосударственные акторы, но под ними в основном понимали противостоящие в вооруженной борьбе за власть внутренние политические силы. Тогда такие противоборства называли конфликтами, не относимыми к войне, зачастую имея в виду гражданские войны, борьбу за национальную независимость и автономию и тому подобное. Активными поборниками противодействия информационной угрозе тогда были, пожалуй, только США — да и то в основном в рамках национальных научных конференций.

Первые разработки в области военных информационных операций также осуществлялись в Соединенных Штатах, где уже начиная с 1993 г. стали готовиться

и публиковаться различного рода военные уставы, наставления, доктрины ведения информационных операций. В 1998 г. Комитет начальников штабов выпустил фундаментальный труд под названием «Объединенная доктрина информационных операций»[4], в котором информационная война получила свое практическое предметное описание. О значении интернета и социальных сетей для активного противоборства в информационном пространстве тогда, по понятным причинам, никто не задумывался, однако *психологические операции* — как тактические, так и стратегические — напрямую относили к информационной сфере.

Спустя годы, в 2004 г. представитель США в Группе правительственных экспертов ООН по международной информационной безопасности заявляла, что никакой угрозы информационной войны нет, а сама информационная война является ничем иным, как химерой. Основной угрозой, с точки зрения Вашингтона, следовало считать киберпреступность. И до сих пор после цветных революций, *Арабской весны* и выявления сложнейших вредоносных программных продуктов, направленных против объектов критической инфраструктуры, Вашингтон продолжает защищать эти же позиции, хотя и более гибко — наличие военной угрозы сегодня все же признается[5].

С тех пор болезнью обеспечения информационной безопасности в той или иной степени заразились многие страны и чуть ли не все международные организации. В настоящее время работает уже третья Группа правительственных экспертов ООН по международной информационной безопасности (ГПЭ МИБ). На протяжении 14 лет ежегодно Генассамблея ООН принимает резолюцию Первого комитета «Достижения в сфере коммуникации и информатизации в контексте международной безопасности», непосредственно посвященную этой проблеме. В течение трех лет по линии Третьего комитета продвигалась резолюция «Культура кибербезопасности». Вопросы информационной безопасности и информационного общества стали постоянными в повестке дня Международного союза электросвязи (МСЭ), под эгидой которого в два этапа, в 2003 и 2005 гг., прошел Всемирный саммит информационного общества — вероятно, самый масштабный форум современности в сфере информационной безопасности. Вопросы информационной безопасности и кибербезопасности значатся в списках важнейших для таких международных организаций, как ШОС, Организация по безопасности и сотрудничеству в Европе (ОБСЕ), Региональный форум Ассоциации государств Юго-Восточной Азии по безопасности (АРФ). Активно работают над военными аспектами данной проблемы НАТО и Организация Договора о коллективной безопасности (ОДКБ). Борьба с терроризмом уже давно не рассматривается иначе как в увязке с вопросами использования интернета в целях пропаганды, рекрутирования новых членов и организации терактов террористическими группами. С передовиц крупнейших СМИ не сходят вопросы киберпреступности. А уж точного числа конференций, симпозиумов, семинаров, круглых столов и иных мероприятий, так или иначе тематически привязанных к повестке информационной безопасности, не знает, вероятно, никто.

Последней каплей для непрофессиональной, но заинтересованной в вопросах информационной безопасности публики должны были бы стать сообщения об упомянутых вредоносных программах, таких как *Stuxnet*, *Duqu*, *Flame*, *Gauss*. Согласно имеющимся на сегодня данным, эти программы якобы способны работать в разных программных средах, распространяясь по интернету, и наносить серьезный физический ущерб вплоть до полного выведения из строя различных, в том числе критических и особо опасных объектов производства, транспорта, энергетики. Информационные системы управления критически важными инфраструктурами стали не только объектами защиты, но и целями для атак. Специалисты предвидели и осознавали эту угрозу еще 20 лет назад, но не смогли объяснить мировому сообществу, что противодействие ей требует, чтобы все информационное пространство (а не только сети связи и технико-программные продукты типа интернета) находилось под национальной и международной защитой.

Постепенно и политологам, и политикам становится ясно, что постиндустриальное общество нуждается не только и не столько в мирном атоме, сколько в мирном информационном пространстве. Договор о нераспространении ядерного оружия (ДНЯО) стал поворотным моментом в истории военной ядерной технологии, нанеся удар по историческому пессимизму и алармизму в международных отношениях. Конечно, заключить аналогичный договор в условиях постиндустриального общества уже вряд ли возможно, но противостояние информационной угрозе, тем не менее, по-прежнему требует многосторонних усилий аналогичного масштаба и глубины. Если это удастся сделать, можно будет констатировать, что человечество осознало бесперспективность насилия в международных отношениях.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — РАЗЛИЧНЫЕ ВЗГЛЯДЫ

Далеко не все сегодня понимают суть и постановку такой задачи одинаково. На сегодняшний день в общем дискурсе об обеспечении международной информационной безопасности четко прослеживаются три направления, которые с известной долей условности можно определить как либеральное, консервативное и прагматическое.

Защитники свободы интернета

В эту широкую группу сегодня попадает большинство интересующихся проблематикой информационной безопасности. Большую долю среди либералов составляет молодежь, в том числе та ее часть, которая в основном умеет только нажимать кнопки на клавиатуре. Теперь с появлением планшетников для многих из них и такое действие стало интеллектуально сложной задачей — достаточно просто провести пальцем по экрану, а вместо писем, которые надо писать, можно обмениваться фотографиями, сделанными при помощи тех же, как теперь все чаще говорят, *гаджетов*. Обмен информацией и доступ к ней видятся представителям данной группы именно в свете особенностей использования ими технологий. В любом случае представители группы либералов — это активные пользователи интернета, по роду своих основных занятий не связанные с деятельностью критических инфраструктур, армией, силовыми и правоохранительными структурами, вопросами, представляющими государственную тайну, и вообще с вопросами функционирования и безопасности государства. Группу объединяет приверженность одному тезису — глобальная сеть должна прежде всего обеспечивать свободу доступа к информации и свободу распространения информации.

О том, что такое информация, все они, как правило, не задумываются. В среде *защитников свободы интернета* считается, что безопасность может достигаться только через абсолютную, никем и ничем не ограниченную свободу. Приверженцев данной точки зрения едва ли беспокоят даже тривиальные вопросы: свобода для кого, свобода от чего, свобода быть или свобода иметь? Возможно, такие вопросы покажутся философскими и отвлеченными от практической дискуссии. Но, не разобравшись, чего же они хотят, сторонники либерального подхода тривиальным образом защищают не свободу и безопасность, а диктат, политическую и финансовую выгоду тех, кто на самом деле контролирует и использует интернет, облегчают жизнь распространителям детской порнографии и инструкций по проведению терактов, торговцам оружием и наиболее опасными товарами и услугами. Никому не хочется таскать каштаны из огня для других, но многие не понимают, что делают именно это.

Но уверены ли они, что Всемирная паутина сейчас действительно свободна, и хотят ли они именно такой свободы для нее в будущем? Интересно, как изменится их риторика в будущем, когда интернет разделится на несколько глобальных сетей. Будет ли входить в их понимание свободы свобода конкуренции новых

сетей друг с другом? Еще одной альтернативой будет фрагментация сети, предполагающая формирование множества зеркал отдельных доменов или их групп, теоретически локализованных в одной стране.

Подлинным жупелом для либералов является угроза контроля над контентом в социальных сетях, и убедить их в том, что подобный контроль не под силу ни одной структуре, даже целому государству, невозможно. Добиться полного контроля не удалось даже в отношении обычной почты, а уж тем более утопично такое предположение в отношении электронных средств, работающих в реальном времени вне географических границ. А в данном случае затрагиваются вопросы соотношения суверенитета, свободы и ответственности. Можно ли решить их в рамках такой концепции? Сомнительно…

Сторонники бумажной информации

Консерваторы, вероятно, решили навсегда заморозить свое сознание на уровне рубежа XIX в., ратуя за безопасный обмен информацией, обеспечение возможности ограничения доступа к документам. Представителей этой группы сегодня уже немного и становится все меньше. Однако, как ни странно, именно глубоко консервативное понимание *информации как документа* закрепляет основная масса правовых норм как в России, так и в других странах.

Консерваторы тоже не всегда знают, чего хотят. Никто не может определить, что такое документ — бумага с текстом или нечто иное? Что является его достаточным признаком — регистрационный номер или же текст? А что делать с чертежами и рисунками? И подобных вопросов масса: является ли документом один лишь номер; как определить, есть ли смысл в тексте или рисунке на документе; и, в итоге, что именно следует сохранять и чем обмениваться при работе с документом? Отсутствие полноценных ответов на эти вопросы подрывает основу взгляда на *информацию как документ*.

Прагматики

Прагматики учитывают все формы существования и перемещения информации и относят информацию к фундаментальным, имманентным бытию, категориям. Я отношу себя к этому течению. На этих позициях изначально стоят военные, относящие к информационным средствам радиоэлектронную борьбу, бомбы — выключатели электричества, химические и биологические средства, приводящие в негодность электронную аппаратуру, психотропные средства и многое другое. Определяющим выступает принцип воздействия на информацию, системы ее обработки, в том числе человеческое сознание, а также системы ее передачи и хранения.

Понятно, что такой подход предполагает существенно более широкое определение информации. Информация как таковая не связана непосредственно с человеком, ее следует рассматривать не только как смысловой результат деятельности мозга, порожденный и локализованный в нем, а как коммуникативную основу любого взаимодействия. Информацией обмениваются все объекты как материального, так и идеального мира, способные к взаимодействию; ее передача и получение возможны в разное время. Информация существует в компьютерных сетях и сетях связи, где человека нет физически и где он не участвует непосредственно в процессе ее передачи. Если учитывать эти утверждения, становится понятно, почему можно обеспечивать целостность и доступность информации в оптических линиях связи, где и электронных импульсов-то нет. Становится легче объяснить, что гены являются носителями информации, а также почему информация выполняет системообразующую функцию и является основой управления в любой сложной системе[6].

АЛОГИЗМЫ?

Три направления, рассмотренные выше, отличаются *подходами* к проблеме информационной безопасности и ставят во главу угла разные ее аспекты: три подхода и три поля борьбы за информационную безопасность и три видения ее задач.

Сторонники *первого подхода* стремятся закрепить или перераспределить права на управление интернетом и в то же время сохранить или перераспределить немалые финансовые потоки, связанные с обладанием этими правами. Именно поэтому основную роль здесь играет МСЭ, один из крупнейших игроков или, точнее, дилеров на этом рынке. Поэтому, не скрывая свой интерес, ему противостоят Соединенные Штаты, создавшие интернет, в значительной степени контролирующие его и не желающие расставаться со своими естественными на него правами. *Второй подход* представляет собой старое и, вероятно, отмирающее направление, которое, как на выборах, скорее отвлекает голоса от *оппозиции*, чем предлагает собственный путь. Под оппозицией, как читатель уже понял, понимаются сторонники *третьего, прагматического подхода*. Российская Федерация здесь играет значительную роль, но на ней список прагматиков не заканчивается. На Всемирном форуме по информационному обществу представители практически всех стран проголосовали за интернационализацию управления интернетом, причем выдвинула эту идею не Россия, а Евросоюз. Представителей ЕС не остановил даже прямой конфликт по этому поводу с присутствовавшей на форуме делегацией *большого брата*.

Однако проблему, по-видимому, следует определять иначе. Интернационализация управления интернетом, безусловно, представляет собой правильный и позитивный процесс, но проблема не в этом. Информационное (не только кибер-[7]) пространство не должно быть уязвимо само по себе и, одновременно, не должно являться источником или каналом реализации военных, террористических или криминальных (неразделимая триада) угроз для других сфер социальной активности человечества. И государство, пока оно является основным членом международного сообщества, должно быть гарантом информационной безопасности и отвечать за действия, совершаемые с его территории или из его информационного пространства. В первую очередь это касается угрозы активного противоборства (то есть военных действий) в информационной сфере. Именно государству общество делегировало функцию обеспечения безопасности, причем не только внешней, но и внутренней.

Противники введения в информационном пространстве каких бы то ни было правил, норм и других ограничений нередко апеллируют к правам человека, в частности к статье 19 Всеобщей декларации прав человека[8], гласящей: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и *свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ* [здесь и далее курсив автора статьи. — *А. Ф.*]».

Однако при этом из аргументации «поборников прав человека в Сети» ускользает тот факт, что предпоследняя 29-я статья Декларации четко показывает, что свобода одного кончается там, где начинается свобода другого. В частности, статья включает следующие положения: «1. Каждый человек имеет обязанности перед обществом, в котором только и возможно свободное и полное развитие его личности. 2. При осуществлении своих прав и свобод каждый человек должен подвергаться только таким *ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе*. 3. *Осуществление этих прав и свобод ни в коем случае не должно противоречить целям и принципам Организации Объединенных Наций*»[9].

Но разве применение информационных средств, как и любых других, в целях войны не противоречит целям и принципам ООН? Или, к примеру, способствует ли укреплению в обществе морали и порядка использование интернета для целей терроризма или распространения детской порнографии? С учетом этого правильнее все-таки воспринимать свободу лучше как осознанную необходимость и именно на этом принципе строить безопасность, в том числе информационную.

И вот здесь появляются те самые алогизмы развития.

Алогизм первый: право информационной войны

Из дискурса об информационной безопасности ушла военная составляющая. По крайней мере, ее не видно: ее не оспаривают, но при этом по существу и не рассматривают. Принятие мер по предотвращению военно-политических угроз информационной безопасности подменяется дискуссиями по мерам доверия в сфере обучения, повышения компьютерного потенциала, сокращения цифрового разрыва и т. п. Вероятно, с начала 1990-х гг. появились более важные и актуальные проблемы. Необходимо поддерживать статус-кво в нынешней расстановке сил в сфере военных информационных разработок, снять с повестки дня вопросы о контроле над производством и принятием на вооружение информационных средств воздействия, интернационализации управления интернетом и завязанных на него потоках денег, сохранить возможность влияния через подконтрольную *всемирную паутину* на социальные группы, СМИ и массовое сознание, вести широкую пропаганду своих идей и ценностей. В случае чего, в кризисной ситуации интернет вместе с GPS можно и отключить. Или наоборот, как это было в Югославии, отключить все, кроме него, а по его каналам доводить до населения и международной общественности *правдивые данные* о враждебном государстве и его структурах и, ломая общественное сознание, уже в потенции исключить противоборство.

Из всех подходов к рассмотрению проблемы военной информационной угрозы выделяется обсуждение применимости международного гуманитарного права к конфликтам в информационном пространстве. Россия всегда придерживалась позиции, что существующее право применимо к информационным операциям, но требует доработки, поскольку формировалось в годы, когда информационные угрозы просто не рассматривались в юридическом ключе[10]. В выпущенном в 1999 г. и переизданном в 2000 г. документе Пентагона было, напротив, четко сказано, что «в настоящее время в международном праве не существует никаких ограничителей на проведение информационных операций»[11]. Осенью 2004 г. в Стокгольме на конференции НАТО[12] с приглашением российской делегации этот же тезис убедительно обосновывался европейскими военными юристами.

Но в 2009 г. в ходе работы второй ГПЭ МИБ правительственный эксперт США вдруг упомянул другой подход, выделив принципы *jus ad bellum*[13] и *jus in bello*[14] как вполне приемлемые для разрешения конфликтов в киберпространстве. После этого все сторонники названных принципов единодушно прозрели и поняли, что современное право вполне применимо к конфликтам в информационном пространстве. И ничего больше не надо, никаких дополнительных соглашений, конвенций, договоров, кодексов — все уже имеется: *jus ad bellum* и *jus in bello* в совокупности полностью покрывают данную проблематику. Остается лишь понять, в чем логика столь внезапного пересмотра подходов, и есть ли она вообще.

Алогизм второй: а о чем вообще речь?

На сегодняшний день информационная безопасность разделилась или, можно сказать, размножилась: появились информационная безопасность бизнеса, информационная безопасность культуры и т.д., однако сущностное наполнение этих концепций зачастую недостаточно и поверхностно, если вообще близко подходит к проблеме информационной безопасности — все чаще встречаются иссле-

дования по вопросам надежности автоматизированных систем вычислительных комплексов или практике журналистики и взаимодействия с общественностью, то есть *не о том*.

Все стремятся обеспечить информационную безопасность, но никто при этом не пытается понять, что такое информация, где она и как существует. Здесь комментировать нечего. Стоит лишь привести в качестве примера подход в целом очень серьезного и интересного издания *Новой философской энциклопедии*[15]. Статья *Информация* этого издания ограничивается отсылкой к статье *Информации теория*[16]. В свою очередь, отсылочная статья гласит, что указанная теория есть «специальная научная дисциплина… анализирующая математические аспекты процессов сбора, передачи, обработки и хранения информации»[17]. Об информации как таковой в ней более не сказано ни слова. Столь же интересна трактовка основного закона в этой области — закона об информации, информационных технологиях и защите информации. Здесь информация определяется как «сведения (сообщения, данные) независимо от формы их представления». При этом, что такое *сведения (сообщения, данные)* в законе не определяется, не говоря уже о том, что эти понятия относятся только к человеческому сознанию.

Аналогичная ситуация наблюдается и за рубежом. Электронный словарь Министерства обороны США, хотя и приводит термины *информационная безопасность, информационная атака, информационная операция* и др., термина *информация* не содержит. Попытка выйти из ситуации через переход к кибербезопасности делает ситуацию абсурдной: выходит, что мы боремся за свободу распространения и доступа к информации, сущность которой не понимаем, и защищаем технические средства и программы.

Алогизм третий: свобода мертвых душ

Как было сказано выше, наиболее многочисленная армия *борцов за информационную безопасность* выступает за свободу интернета, яростно отстаивая мысль о том, что глобальная сеть — это новый мир, который сформировал новую интернет-культуру. Но кто граждане этого мира? Передовая личность ассоциируется теперь с блогером, каждый уважающий себя человек, в том числе президент, имеет собственный блог, притом что еще пять лет назад в лучшем случае имел домашнюю страницу, а о блогах вообще никто не знал. Формируется представление, что весь мир завязан на интернет и блогосферу. Однако при серьезном обсуждении все специалисты в информационной безопасности в один голос говорят, что ни в одной из критических инфраструктур интернета нет — даже в серьезном бизнесе он кончается там, где кончаются отношения с клиентом. А интернет, по большому счету, — это только социальные сети.

Тогда какую же свободу столь бескомпромиссно защищают информационные либералы — свободу социальных сетей? И как много реальных интернет-пользователей? Как их подсчитывать? По IP-адресам, *никнеймам*? Или те, кто считает, имеют средства узнать, сколько у каждого человека адресов и имен в сети? А как, к примеру, считать тех активных пользователей, которых в период событий *Арабской весны* тысячами создавали специальные программы? Если признать их *мертвыми душами*, то следует отметить и то, что современные политические Чичиковы оказались гораздо более удачливы, чем герой Гоголя. Интернет–души не только продают и покупают, опираясь на их мнение и голоса, но и строят нужную международную политику, меняют неугодные режимы.

Алогизм четвертый: информация VS суверенитет

Информационная безопасность зачастую воспринимается как выражение антипода свободы распространения и доступа к информации.

Любое общество становится организованным лишь тогда, когда его члены начинают действовать в рамках выработанной им системы права. Основой общественной организации всегда являются нормы поведения и их сознательное выполнение. Однако в сфере международной информационной безопасности наблюдается, напротив, отрицание самой возможности введения норм и правил поведения государств и других субъектов отношений. Взамен предлагается *культура кибербезопасности*, а по сути — *альтруизма*.

В современном международно-политическом дискурсе по непонятным причинам противопоставляются идеи суверенитета государства над своим информационным пространством и ответственности государства за действия, совершенные из его информационного пространства. Общеизвестно, что обязанности могут основываться только на правах, и наоборот. Каким образом нести ответственность за что-то, над чем не имеешь прав суверенного контроля, в отсутствие которого ответственность также не может быть единоличной (а в нашем случае — *единогосударственной*)? Если установленный злоумышленник для интернет-атаки создал бот-сеть, размещенную на ресурсах десятка стран, должны ли эти страны также нести ответственность за его действия? Особенность метода создания бот-сетей заключается как раз в том, что владелец ресурсов не подозревает об их использовании злоумышленником. Чтобы отвечать за такого пользователя, государство, как минимум, должно располагать правом принуждения его к культуре кибербезопасности и использованию соответствующих средств контроля, которые могут быть помехой пользователю в его бизнесе, но он, тем не менее, будет обязан (по закону!) их исполнять.

Разве это — не одно из проявлений суверенитета? И наоборот, разве суверенитет не предполагает ответственность суверена за любые действия в тех сферах, на которые распространяются его суверенные права? Весьма уместно здесь было бы принятие кодекса поведения стран в информационном пространстве. Идея разработки такого кодекса присутствует и в разработанной администрацией США и презентованной Бараком Обамой 22 мая 2011 г. Международной стратегии по действиям в киберпространстве. Основой для кодекса вполне могли бы послужить предложенные четырьмя странами ШОС на 66-й сессии Генассамблеи ООН Правила поведения в области международной информационной безопасности[18]. Такой документ мог бы стать основой для внедрения на международном уровне культуры кибербезопасности, которая естественным образом проецировалась бы на национальный уровень. Однако и эта идея упорно отклоняется. Не совсем ясно, в чем заключается логика таких действий.

Алогизм пятый: противоречия в идеях теоретиков либерального лагеря

Либералы выступают категорически против отнесения социальной сферы к области информационной безопасности, однако при этом делают акцент на интернете и социальных сетях. Ни у кого не вызывает сомнений, что демократическое государство существует, для того чтобы обеспечивать государственную и общественную безопасность и, в частности надежную работу критических инфраструктур, — это его основные функции, именно эти права ему делегировало общество, и вопрос о суверенитете в данном случае никем не поднимается.

При этом появление таких убедительных свидетельств военного применения информационных технологий, как *Stuxnet*, *Duqu*, *Flame* и *Gauss*, не изменило акцентов дискуссии. Военные эксперты США и России включили появление *Stuxnet* в десятку самых серьезных военных событий 2010 г., причем отнюдь не в конце списка. В ответ прозвучали лишь разрозненные голоса, напомнившие, что в тех областях, где подобные *Stuxnet* средства могут нанести наибольший ущерб (управление технологическим процессом на крупных и особо опасных производствах, в энергетике, транспорте и пр.) обеспечить безопасность в настоящее время может только государство и только на основе суверенных прав. В данном случае такие фундаментальные права человека, как право на доступ к информа-

ции и право на распространение информации, за которые так радеют либералы, никак не ущемляются. Интересно, а как они мыслят его реализацию в системе, например, трансконтинентального нефтепровода или АЭС? Следуя такой логике, правила дорожного движения ущемляют фундаментальное право свободы передвижения и противоречат интересам развития, ограничивая мобильность рабочей силы. И если, к примеру, предложение передать функции обеспечения защиты от ракетно-ядерной угрозы от вооруженных сил обществу будет воспринято не иначе как признак серьезного заболевания, то почему в отношении информационной безопасности предлагается устранить государство и руководствоваться лозунгом «спасение утопающих — дело рук самих утопающих»?

Можно продолжать и далее, но и без того очевидно, что построение логичной и адекватной концепции информационной безопасности для использования в международных и общественных отношениях еще далеко до завершения.

***

Уже почти 15 лет Россия и мировое научное сообщество[19] прилагают значительные усилия к тому, чтобы предотвратить превращение информационного пространства, ставшего одной из ключевых критических инфраструктур человечества, в поле боя. В целом эту же цель поставила перед собой и ООН. Однако — и это тоже следует признать — ее достижение пока не просматривается.

Главный вопрос информационной безопасности, наверное, можно было сформулировать как классическую философскую антитезу бытия: «Человек с оружием или человек с орудием». Было бы правильно, если бы идея международной информационной безопасности стала основой философии мира в постмодерне, а не постиндустриальным вариантом идеи противостояния войне. Но пока, к сожалению, информационная безопасность в общественном дискурсе выглядит некоей совокупностью бодрияровских симулякров, которые вытесняют и подменяют собой собственные смыслы рассматриваемых проблем.

Александр Федоров,
член Экспертно-консультативного совета ПИР-Центра
fedorov-av@bk.ru

Примечания

[1] Источник цитаты умышленно не приводится, дабы не ставить специалистов данной страны в неудобное положение, однако речь идет о документе 2012 г., который имеется в распоряжении автора; в тексте дается точное цитирование.

[2] Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. (Екатеринбург. 16.06.2009.) Текст имеется в распоряжении ПИР-Центра.

[3] Этот термин также продолжает существовать и не только в российской терминологии. Современный электронный словарь военных терминов Министерства обороны США (http://www.dtic.mil/doctrine/dod_dictionary/, последнее посещение — 3 сентября 2012 г.) дает не совпадающую с российской, но вполне приемлемую дефиницию этого термина: *информационная безопасность* — защита информации и информационных систем от несанкционированного доступа или модификации информации при ее хранении, обработке или транзите от отказа в обслуживании зарегистрированным пользователям. (Источником указан документ, приведенный в следующей сноске).

[4] Joint doctrine for information operations, JCS, Joint Pub 3–13, 8 October 1998.

[5] Надо полагать, из Вашингтона мониторинг военных угроз вести сподручнее. Если верить еженедельнику Jane's Defense Weekly (цитируется по «Пентагон принимает «План X». *Красная Звезда.* 2012, 25 августа. № 155) только по линии DARPA [Агентство передовых обо-

ронных исследовательских проектов] на разработки в области кибертехнологий Пентагону в 2012 г. выделено 208 млн долл.

[6] См. подробнее: Расторгуев С. П. Философия информационной войны. М.: Психолого-социальный институт, 2003.

[7] Если следовать американской официальной логике, киберпространство представляет собой систему открытых сетей связи и подключенных к ним компьютеров с соответствующим программным обеспечением, то есть *интернет без информации и пользователей*. Кибербезопасность включает безопасность сетей связи, компьютеров и программного обеспечения для их функционирования. Информационное пространство понимается как совокупность всех сфер применения информационно-телекоммуникационных средств и технологий (ИКТ), обрабатываемая в них информация и люди, занятые в этой среде. Словарь военных терминов Министерства обороны США определяет киберпространство как «глобальную область в пределах информационной окружающей среды, состоящей из взаимосвязанной сети информационных инфраструктур и технологии, включая Интернет, телекоммуникационные сети, компьютерные системы, и вложенные процессоры и диспетчеров». Примечательно, что термин *кибербезопасность* словарь Минобороны США не содержит. Соответственно, понимание информационной безопасности даже в американской военной трактовке оказывается существенно более широким и содержательно наполненным и действительно может рассматриваться как безопасность информационного общества, где все основные сферы деятельности самым непосредственным образом основаны на ИКТ.

[8] Всеобщая декларация прав человека. Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 г. Декларации. Организация Объединенных Наций, http://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (последнее посещение — 9 октября 2012 г.).

[9] Там же, Статья 29.

[10] Одним из первых экспертных центров, выдвинувших такой подход, был ПИР-Центр, который в 2001 г. опубликовал следующую монографию, содержавшую соответствующие разделы:

И. Ю. Алексеева и др. Информационные вызовы национальной и международной безопасности. Под общ. редакцией А. В. Федорова и В. Н. Цыгичко — М.: ПИР-Центр, 2001.

[11] An Assessment of International Legal Issues in Information Operations, DOD, March 1999.

[12] International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17–19 November 2004.

[13] Право объявлять войну как часть международного права в области прав человека.

[14] Право войны или право вооруженных конфликтов.

[15] Новая философская энциклопедия в 4-х томах. М.: Мысль, 2001.

[16] Там же. С. 143.

[17] Там же. С. 141.

[18] Документ 66-й сессии Генеральной ассамблеи ООН А/66/359, распространен 14 сентября 2011 г.

[19] В 1999 г. Всемирная конфедерация ученых на ежегодной конференции в Эриче (Италия) признала, что в XXI в. основные угрозы человечеству будут носить информационный характер.

SUMMARY

FROM THE EDITOR

INTERVIEW

Бейсли-Уокер Бен — руководитель Программы по новым угрозам безопасности в Институте ООН по вопросам разоружения (ЮНИДИР) с 2011 г. Окончил Международный космический университет (ISU), Университеты Эдинбурга и Амстердама. Ранее работал в должности Советника по политике безопасности и международному праву в фонде «Безопасный мир» (Secure World Foundation). Занимал пост председателя неправительственной организации *Консультативный совет космического поколения* (Space Generation Advisory Council). В 2010–2011 гг. принимал участие в работе различных форумов и площадок ООН, включая Комиссию ООН по мирному использованию открытого космоса (UNCOPUOS), Конференцию по разоружению, а также Генеральную Ассамблею ООН. В рамках этого направления деятельности в 2009 г. впервые представил от лица неправительственной организации презентацию по проблемам безопасности космоса в рамках неформальной пленарной сессии Конференции по разоружению. Адрес электронной почты: *bbaseleywalker@unog.ch.*

Боммелер Констанс — директор по государственной политике Общества Интернета (ISOC), работает над развитием сотрудничества с международными организациями, а также выработкой стратегических позиций ISOC по вопросам, связанным с интернетом. В рамках данной должности основала и в настоящее время координирует деятельность Технического консультативного совета по вопросам Интернета (ITAC) для Организации экономического сотрудничества и развития (ОЭСР). Также координирует взаимодействие ISOC с Организацией Объединенных Наций по вопросам Образования, Науки и Культуры (ЮНЕСКО), Всемирной организацией интеллектуальной собственности (ВОИС), а также *Большой восьмеркой, Большой двадцаткой* и международными Форумами по управлению интернетом (IGF). В 2010–2011 гг. отвечала за стратегическое развитие Программы ISOC «Лидеры нового поколения», нацеленной на подготовку юных профессионалов со всего мира к роли новых лидеров в области интернет-технологий, политики и бизнеса. Принимала участие в работе Всемирного саммита информационного общества (WSIS), в 2007–2008 гг. содействовала развитию сотрудничества в правовой и технической плоскости между Францией и государствами Африки в рамках проекта борьбы со спамом Signal Spam. Адрес электронной почты: *bommelaer@isoc.org.*

Васильев Виктор Львович — заместитель Постоянного представителя России при Отделении Организации Объединенных Наций и других международных организациях в Женеве. В 1989–1993 гг. работал в Москве в Министерстве иностранных дел СССР (России). В 1993–1997 и 2000–2004 гг. занимал различные посты в Постоянном представительстве России при международных организациях в Нью-Йорке, получил ранг старшего советника по политическим вопросам (со специализацией на Совете Безопасности). С 2004 по 2007 г. работал в качестве заместителя директора Департамента международных организаций МИД России. Участво-

вал в работе нескольких советских и, затем, российских делегаций по различным вопросам международной повестки дня, включая Обзорные конференции ДНЯО 1995, 2000 и 2005 гг., сессии Комиссии ООН по разоружению и т. п. В 2005–2006 гг. был правительственным экспертом Группы правительственных экспертов по всем аспектам верификации. Ныне является также членом Группы правительственных экспертов по проблеме милитаризации космического пространства. Адрес электронной почты: *rus.disarm@gmail.com.*

Вебер Рольф — заведующий кафедрой права, профессор права Гарвардской школы права. С 1995 г. профессор кафедры гражданского, коммерческого и европейского права Университета Цюриха и приглашенный профессор в Университете Гонконга, преподает и публикуется в области гражданского, коммерческого и европейского права в области интернета, средств информации и конкуренции, международных финансов и торгового регулирования. Член Европейского диалога по вопросам управления интернетом (EuroDIG) Также является директором Европейского института права и Центра информационного и коммуникационного права в университете Цюриха. Член руководства аспирантуры в области международного бизнес-права и программы МБА в Университете Цюриха. С 2008 г. является членом организационного комитета Академической сети по глобальному управлению интернетом (GigaNet) и с 2009 г. — членом Группы советников Глобального альянса за информационно-коммуникационные технологии и развитие (GAID). Адрес электронной почты: *rolf.weber@rwi.unizh.ch.*

Демидов Олег Викторович — научный сотрудник ПИР-Центра, координатор проекта ПИР-Центра «Международная информационная безопасность и глобальное управление интернетом». В 2010 г. окончил факультет государственного управления МГУ имени М. В. Ломоносова. С 2011 г. занимает должность координатора проектов Центра политических и международных исследований (ЦПМИ). Аспирант кафедры политической теории Московского государственного института международных отношений (Университета) МИД РФ. Участник международных конференций по вопросам кибербезопасности, управления интернетом, урегулирования региональных конфликтов. С 2011 г. участник проекта Франкфуртского института исследования проблем мира и конфликтов *Посттрансатлантическая эпоха: Новый концерт великих держав в XXI в.* Выпускник Международной летней школы по проблемам международной безопасности ПИР-Центра (2012). Адрес электронной почты: *demidov@pircenter.org.*

Зиновьева Елена Сергеевна — старший преподаватель кафедры мировых политических процессов Московского государственного института международных отношений (Университета) МИД РФ с 2009 г., кандидат политических наук (2009). С 2007 по 2009 г. — аспирант кафедры мировых политических процессов МГИМО (У) МИД РФ. Победитель конкурса ректорских грантов. С 2007 по 2008 г. — сотрудник Центра интернет-политики МГИМО (У) МИД РФ. В 2009–2011 гг. была исполнителем научного проекта «Динамика мирового политического развития и проблемы глобальной конкурентоспособности России» Министерства образования и науки РФ, НОЦ МГИМО (У) МИД России. В настоящее время (2012–2013 гг.) является исполнителем научных проектов РГНФ 12-03-00649 «Теория и практика межкультурного взаимодействия в контексте европейской безопасности», а также РГНФ 12-06-00869 «Социально-психологический анализ российской научно-исследовательской культуры (на основе данных исследования экспертных процедур российских фондов поддержки науки)». Адрес электронной почты: *zinovjeva.elena@gmail.com.*

Ибрагимова Галия Ринатовна — консультант ПИР-Центра, представитель журнала *Индекс Безопасности* в Ташкенте. В июле 2012 г. защитила диссертацию на соискание ученой степени кандидата политических наук на тему «Глобальное информационное пространство в условиях формирования нового мирового порядка» при Университете мировой экономики и дипломатии (Ташкент, Узбекистан). Выпускница магистратуры отделения международной журналистики факультета международных отношений УМЭД. В 2008–2009 гг. прошла интенсивный курс по программе MBA в Узбекско-японском центре развития человеческих ресурсов с присвоением международной степени Project Management Professional (PMP). Участница ряда конференций по проблемам региональной безопасности в Центральной Азии.

Выпускница Международной летней школы по проблемам международной безопасности (2008). Адрес электронной почты: *ibragimova@pircenter.org.*

Касенова Мадина Балташевна — профессор кафедры международного частного права Дипломатической академии МИД России, кандидат юридических наук (1987). Выпускница юридического факультета Московского государственного университета имени М.В. Ломоносова. Сотрудник Торгово-промышленной палаты СССР/России (1989–1993), член Рабочей группы по правовым вопросам Совета делового сотрудничества СССР–Канада (1990–1992 гг.), главный эксперт при руководстве Международной ассоциации штрихового кодирования ЮНИСКАН, член российских официальных делегаций на международных межправительственных конференциях, участница международных конференций, а также переговоров по вопросам инвестиционного сотрудничества, адвокат Международной юридической фирмы *Бейкер и Макензи* (1992–1995 гг.), заведующая юридической консультацией № 2 коллегии адвокатов *Инюрколлегия* (2001–2003 гг.). Адрес электронной почты: *mkassenova@gmail.com.*

Куммер Маркус — вице-президент Общества Интернета (ISOC) по государственной политике с 2011 г. До января 2011 гг. занимал позицию исполнительного директора Секретариата форума управления интернетом (IGF), будучи назначен на пост Генеральным секретарем Организации Объединенных Наций в 2006 г. Ранее возглавлял секретариат Рабочей группы по управлению Интернетом (WGIG), учрежденной Генеральным секретарем ООН по результатам Первого этапа Всемирного саммита по информационному обществу (WSIS). С 2002 по 2004 г. занимал пост Уполномоченного по электронным службам (eEnvoy) Министерства иностранных дел Швейцарии в Берне. В основные задачи входила координация международной политики в области информационно-коммуникационных технологий в целом и WSIS в частности. Был членом делегации Швейцарии во время первого этапа WSIS, где он руководил работой нескольких переговорных групп, включая группу по управлению интернетом. Кадровый дипломат, служил в нескольких миссиях Министерства иностранных дел Швейцарии в Берне, Лиссабоне, Вене, Осло, Женеве и Анкаре. Адрес электронной почты: *kummer@isoc.org.*

Орлов Владимир Андреевич — президент ПИР-Центра, главный редактор журнала *Индекс Безопасности*. Является основателем (1994 г.) и бессменным президентом ПИР-Центра. С 2006 г. возглавляет Европейское отделение ПИР-Центра в Женеве — Centre russe d'etudes politiques. Является членом Совета ПИР-Центра. Член Российского Пагуошского комитета при Президиуме РАН. Член Научного совета при Национальном комитете по исследованию БРИКС. Член Монтерейской группы по разработке стратегии в области нераспространения. Член Редакционной коллегии журнала *Washington Quarterly*. Основатель (1993 г.), член Международного клуба *Триалог*. Ассоциированный научный сотрудник Женевского центра политики безопасности (GCSP). Член делегации Российской Федерации на Обзорной конференции ДНЯО. Член Международной академии по ядерной энергии (INEA). Кандидат политических наук. Под его общей редакцией был издан учебник *Ядерное нераспространение* (второе издание — 2003 г.). Адрес электронной почты: *orlov@pircenter.org.*

Пондер Ярослав — Советник по вопросам стратегии и политики в Международном союзе электросвязи (МСЭ); работает в МСЭ с 2004 г. Защитил кандидатскую степень по бизнес-менеджменту и управлению (МАА), а также по управлению проектами (DAS) в Университете Женевы (Швейцария); в настоящее время участвует в программе на соискание докторской степени в области бизнеса и управления для руководителей в Университете Париж–Дофин (Paris IX). С 1999 по 2003 г. работал в Европейском институте международных экономических отношений в Потсдаме и Вуппертале, Германия. С 2005 г. работал в качестве Советника по вопросам стратегии и политики, а также руководителя ряда проектов в МСЭ, в 2007 г. перешел в Департамент проектов и инициатив Бюро развития электросвязи МСЭ (БРЭ). В 2008 г. был назначен координатором МСЭ для стран Европы, осуществив на этом посту успешную координацию деятельности МСЭ в регионе. В 2009 г. был переведен в Генеральный секретариат МСЭ в качестве координатора по вопросам стратегии и политики. В рамках своей деятельности уделял первоочередное внимание разработке стратегии эффективной реализации положений Всемирного

саммита информационного общества. В 2010 г. был повышен до позиции советника по вопросам стратегии и политики. В октябре 2011 г. в дополнение к текущим должностным позициям вновь получил дополнительные обязанности координатора МСЭ для стран Европейского региона, включающего 43 государства. Адрес электронной почты: *jaroslaw.ponder@itu.int.*

Сикорская Надежда Александровна — главный редактор электронного издания *Наша Газета.ch.* Окончила факультет журналистики Московского государственного университета (1990), кандидат исторических наук (1994). Начала профессиональную деятельность как переводчик в Министерстве культуры СССР, затем посвятила 13 лет работе в ЮНЕСКО (в Париже и Женеве). В круг обязанностей входили различные сюжеты от продвижения Всемирной конвенции по охране культурного и природного наследия и создания международной программы грантов для творческой молодежи до редактирования международного журнала по вопросам образования. Расставшись с ЮНЕСКО в 2004 г., Надежда работала директором по связям с общественностью в Международном Зеленом Кресте, неправительственной организации, созданной и возглавляемой Михаилом Горбачевым. В 2007 г. приступила к обязанностям главного редактора издания НашаГазета.ch. Адрес электронной почты: *nadia.sikorsky@nashagazeta.ch.*

Симоненко Максим Дмитриевич — студент магистерской программы *Международные отношения: азиатские исследования* факультета мировой экономики и мировой политики Национального исследовательского университета Высшая школа экономики (НИУ ВШЭ). Выпускник отделения международных отношений исторического факультета Томского государственного университета (ТГУ) (2011). Участник IV (2009) и V (2010) Летних школ по проблемам нераспространения ядерного оружия, организованных Томским государственным университетом и Шведским управлением по радиационной безопасности. С мая по август 2012 г. прошел стажировку в ПИР-Центре. Адрес электронной почты: *simonenko.maksim@gmail.com.*

Федоров Александр Валентинович — член Экспертно-консультативного совета ПИР-Центра. Окончил Московский государственный университет имени М. В. Ломоносова и аспирантуру МГУ. Имеет ученую степень кандидата физико-математических наук и ученое звание старшего научного сотрудника. После окончания учебы работал в учреждениях государственного аппарата. Занимался проблемами разоружения и нераспространения ОМУ. Последние 15 лет ведет активную научную и практическую деятельность в сфере международной информационной безопасности и противодействия высокотехнологичному терроризму. Входил в состав российских делегаций на многих международных форумах по этой проблематике в форматах ООН, G8, Совета Европы, ШОС и др. Профессор кафедры мировых политических процессов МГИМО (У) МИД РФ. Входил в состав экспертного совета Комитета по безопасности Государственной думы 4-го созыва. Советник директора Института проблем информационной безопасности МГУ имени М. В. Ломоносова. Автор около 100 научных публикаций в российских и зарубежных изданиях. Адрес электронной почты: *fedorov-av@bk.ru.*

Якушев Михаил Владимирович — председатель Совета ПИР-Центра (с 2010 г.), также занимает пост вице-президента MailRu Group (с 2012 г.). Был представителем Российской Федерации в Рабочей группе по управлению интернетом при Генеральном секретаре ООН (2004–2005 гг.). В 2009–2011 гг. — заместитель председателя Рабочей группы Совета Европы по вопросам трансграничного Интернета. В 2008–2010 гг. был председателем Совета Координационного центра национального домена сети Интернет .RU. Окончил Московский государственный институт международных отношений МИД СССР по специальности «международное право» в 1989 г. С 1997 г. возглавлял юридические службы российских представительств международных компаний в области телекоммуникационных и информационных технологий. В 2000–2001 гг. — представитель Российской Федерации в Рабочей группе *Группы восьми* по возможностям информационного общества (DOT Force), в 2004–2006 гг. — директор Департамента правового обеспечения Министерства информационных технологий и связи Российской Федерации. С 2010 г. преподает на кафедре международного частного права Дипломатической академии МИД РФ. Адрес электронной почты: *m.yakushev@gmail.com.*

ЭКСПЕРТНО-КОНСУЛЬТАТИВНЫЙ СОВЕТ ПИР-ЦЕНТРА

(по состоянию на 25 октября 2012 г.)

Айнхорн Роберт, старший советник по вопросам нераспространения и контроля над вооружениями, Госдепартамент, Вашингтон, США

Академия ОБСЕ, Бишкек, Киргизия

Антипов Сергей Викторович, д.т.н., заместитель директора, Институт безопасного развития атомной энергетики РАН, Москва, Россия

Антонов Анатолий Иванович, Чрезвычайный и Полномочный Посол, к.э.н., заместитель министра, Министерство обороны Российской Федерации, Москва, Россия

Арбатов Алексей Георгиевич, д.и.н., академик РАН, руководитель, Центр международной безопасности, ИМЭМО РАН, Москва, Россия

Ахтамзян Ильдар Абдулханович, к.и.н., доцент, кафедра международных отношений и внешней политики России, МГИМО МИД РФ, Москва, Россия

Баев Павел Кимович, к.и.н., проф., Международный институт исследований проблем мира, Осло, Норвегия

Барановский Владимир Георгиевич, д.и.н., проф., академик РАН, заместитель директора, ИМЭМО РАН, Москва, Россия

Всероссийский научно-исследовательский институт технической физики им. акад. Е. И. Забабахина (ВНИИТФ), Российский федеральный ядерный центр, Снежинск, Россия

Всероссийский научно-исследовательский институт экспериментальной физики (ВНИИЭФ), Российский федеральный ядерный центр, Саров, Россия

Воронков Владимир Иванович, к.и.н., постоянный представитель, Представительство России при международных организациях в Вене, Вена, Австрия

Готтемюллер Роуз, заместитель госсекретаря США, Вашингтон, США

Данапала Джаянта, посол, президент, Пагуошское движение ученых, председатель, Совет Университета ООН, Коломбо, Шри-Ланка

Данилов Дмитрий Александрович, к.э.н., проф., ведущий научный сотрудник, заведующий, Отдел европейской безопасности, Институт Европы РАН, Москва, Россия

Дворкин Владимир Зиновьевич, д.т.н., генерал-майор (в отставке), главный научный сотрудник, ИМЭМО РАН, Москва, Россия

Джонсон Ребекка, д-р, исполнительный директор, Институт *Акроним*, Лондон, Великобритания

Евстафьев Дмитрий Геннадьевич, к.п.н., директор, Департамент стратегии коммуникаций, управление общественных связей, TNK BP, Москва, Россия

Елеукенов Дастан Шериазданович, д. ф.-м. н., советник, посольство Республики Казахстан в США, Вашингтон, США

Есин Виктор Иванович, к.в.н., проф., генерал-полковник (в отставке), консультант командующего ракетными войсками стратегического назначения, Министерство обороны РФ, Москва, Россия

Женевский центр политики безопасности, Женева, Швейцария

Институт стратегической стабильности, Москва, Россия

Кириченко Элина Всеволодовна, к.э.н., руководитель, Центр североамериканских исследований, ИМЭМО РАН, Москва, Россия

Кожокин Евгений Михайлович, д.и.н., ректор, Академия труда и социальных отношений, Москва, Россия

Кортунов Андрей Вадимович, к.и.н., генеральный директор, Российский совет по международным делам, Москва, Россия

Краснов Алексей Борисович, начальник управления, Управление пилотируемых программ, Федеральное космическое агентство, Москва, Россия

Лаверов Николай Павлович, д. г.-м. н., проф., академик РАН, вице-президент, Российская академия наук, Москва, Россия

Ладыгин Федор Иванович, генерал-полковник (в отставке), советник генерального директора, Авиационная холдинговая компания *Сухой*, Москва, Россия

Лебедев Владимир Владимирович, заместитель руководителя департамента, Департамент внешнеэкономических и международных связей, правительство Москвы, Москва, Россия

Лукьянов Федор Александрович, главный редактор, журнал *Россия в глобальной политике*, Москва, Россия

Лысенко Михаил Николаевич, Чрезвычайный и Полномочный Посол, директор, Департамент международного сотрудничества, Государственная корпорация по атомной энергии *Росатом*, Москва, Россия

Льюис Патриция, д-р, директор по исследованиям, *Chatham House*, Лондон, Великобритания

Маргелов Михаил Витальевич, председатель, Комитет по международным делам, Совет Федерации ФС РФ, Москва, Россия

Международная жизнь, журнал, Москва, Россия

Московский государственный институт международных отношений (Университет) МИД РФ, Москва, Россия

Мурогов Виктор Михайлович, проф., Государственный технический университет атомной энергетики, Обнинск, Россия

Мурсанков Сергей Геннадьевич, заместитель директора, аналитический центр, ОАО «Объединенная авиастроительная корпорация», Москва, Россия

Мюллер Харальд, д-р, проф., директор, Институт проблем мира, Франкфурт, Германия

Мясников Евгений Владимирович, директор, Центр по изучению проблем контроля над вооружениями, энергетики и экологии, Долгопрудный, Россия

Национальный исследовательский ядерный университет «МИФИ», Москва, Россия

Никитин Александр Иванович, д.п.н., проф., директор, Центр политических и международных исследований, Москва, Россия

Новиков Владимир Евгеньевич, к.э.н., заместитель начальника, отдел оборонной политики, Российский институт стратегических исследований, Москва, Россия

Пархалина Татьяна Глебовна, к.и.н., заместитель директора, ИНИОН РАН, директор, Центр по изучению проблем европейской безопасности ИНИОН РАН, Москва, Россия

Пономарев-Степной Николай Николаевич, д.т.н., проф., академик РАН, Москва, Россия

Радчук Александр Васильевич, к.т.н., советник начальника Генерального штаба Вооруженных сил РФ, Москва, Россия

Решетников Леонид Петрович, к.и.н., генерал-лейтенант, директор, Российский институт стратегических исследований (РИСИ), Москва, Россия

РНЦ *Курчатовский институт*, Москва, Россия

Рогачев Илья Игоревич, директор, Департамент по вопросам новых вызовов и угроз, МИД России, Москва, Россия

Рыбаченков Владимир Иванович, к.т.н., ведущий научный сотрудник, Центр по изучению проблем контроля над вооружениями, энергетики и экологии, Долгопрудный, Россия

Савельев Александр Георгиевич, д.п.н., заведующий, отдел стратегических исследований, Центр международной безопасности, ИМЭМО РАН, Москва, Россия

Сатановский Евгений Янович, к.э.н., проф., президент, Институт Ближнего Востока, Москва, Россия

Семин Валерий Витальевич, д.т.н., проф., старший советник, Постоянное представительство РФ при НАТО, Брюссель, Бельгия

Сиринционе Джозеф, президент, Фонд Плаушерс, Вашингтон, США

Соков Николай Николаевич, к.и.н., д.п.н., старший научный сотрудник, Венский центр изучения проблем разоружения и нераспространения, Вена, Австрия

Сумский Виктор Владимирович, д.и.н., директор, Центр АСЕАН при МГИМО (У) МИД РФ, Москва, Россия

Тимербаев Роланд Михайлович, Чрезвычайный и Полномочный Посол, д.и.н., профессор, Москва, Россия

Тренин Дмитрий Витальевич, к.и.н., директор, Московский центр Карнеги, Москва, Россия

Трубников Вячеслав Иванович, генерал армии, член дирекции, ИМЭМО РАН, Москва, Россия

Тузмухамедов Бахтияр Раисович, к.ю.н., проф., судья Международного уголовного трибунала по Руанде, советник, Управление международного права, Конституционный суд РФ, Москва, Россия

Убеев Алексей Вадимович, к.т.н., главный специалист, Офис ядерной безопасности, Департамент ядерной безопасности и физической защиты, Международное агентство по атомной энергии, Вена, Австрия

Федоров Александр Валентинович, к. ф.-м. н., эксперт, Служба внешней разведки, Москва, Россия

Федоров Валерий Валерьевич, к.п.н., генеральный директор, Всероссийский центр изучения общественного мнения, Москва, Россия

Феоктистов Дмитрий Валериевич, к.и.н., заместитель директора, Департамент по вопросам новых вызовов и угроз, МИД РФ, Москва, Россия

Фонд нераспространения во имя глобальной безопасности, Буэнос-Айрес, Аргентина

Хлопков Антон Викторович, директор, Центр энергетики и безопасности, Москва, Россия

Цзи Чжие, вице-президент, Китайская академия современных международных отношений, Пекин, КНР

Эггерт Константин фон, политический обозреватель, радио *КоммерсантЪ FM*, Москва, Россия

СОВЕТ ПО УСТОЙЧИВОМУ ПАРТНЕРСТВУ С РОССИЕЙ

(по состоянию на 25 октября 2012 г.)

Антонов Анатолий Иванович, Чрезвычайный и Полномочный Посол, к.э.н., заместитель министра, Министерство обороны РФ, Москва, Россия

Бужинский Евгений Петрович, генерал-лейтенант (запаса), старший вице-президент, ПИР-Центр, Москва, Россия

Ганкин Леонид Эммануилович, департамент по международным отношениям и связям с общественностью, Фонд *Сколково,* Москва, Россия

Зевелев Игорь Александрович, д.п.н., директор Московского филиала, Фонд Макартуров, Москва, Россия

Орлов Владимир Андреевич, к.п.н., президент, ПИР-Центр, Москва, Россия

Пайфер Стивен, посол, старший научный сотрудник, Институт Брукингса, Вашингтон, США

Сиринционе Джозеф, президент, Фонд Плаушерс, Вашингтон, США

Скуазони Шэрон, директор, старший научный сотрудник, Программа по предотвращению распространения, Центр стратегических и международных исследований, Вашингтон, США

Спасский Николай Николаевич, к.и.н., д.п.н., Чрезвычайный и Полночный Посол, заместитель генерального директора, Государственная корпорация по атомной энергии *Росатом,* Москва, Россия

Холловэй Дэвид, д-р, проф., член Совета директоров, Фонд Плаушерс, Сан-Франциско, США

Хоффман Дэвид, внештатный редактор газеты *Вашингтон Пост*, Вашингтон, США

Эллеман Майкл, старший научный сотрудник, Международный институт стратегических исследований, Манама, Бахрейн

МЕЖДУНАРОДНАЯ ЭКСПЕРТНАЯ ГРУППА

(по состоянию на 25 октября 2012 г.)

Аргуэльо Ирма, основатель и руководитель, Фонд нераспространения во имя глобальной безопасности, Буэнос-Айрес, Аргентина

Бенаму Мухаммед, президент Марокканского центра стратегических исследований, Рабат, Марроко

Бужинский Евгений Петрович, генерал-лейтенант, старший вице-президент ПИР-Центра, Москва, Россия

Джаятиллека Дайан, Посол Шри-Ланки во Франции, постоянный представитель Шри-Ланки при ЮНЕСКО, Париж, Франция

Дуарте Сержио, высокий представитель Генерального секретаря ООН по вопросам разоружения (2007–2012 гг.), Рио-де-Жанейро, Бразилия

Дунай Пал, руководитель программы по международной безопасности, Женевский центр политики безопасности, Женева, Швейцария

Каравели Халил, руководитель проекта по Турции, Институт по изучению Центральной Азии и Кавказа при университете Джона Хопкинса, Анкара, Турция

Кортунов Андрей Вадимович, к.и.н., генеральный директор, Российский совет по международным делам, Москва, Россия

Макгетланенг Сехларе, д.п.н., директор, Программа государственного управления и демократии, Южноафриканский институт африканских исследований, Претория, ЮАР

Мехди Санаи, доктор политологии, директор, Институт исследования Ирана и Евразии, Тегеран, Иран

Поттер Уильям, проф., директор, Центр исследования проблем нераспространения им. Джеймса Мартина, Монтерейский институт международных исследований, Монтерей, США

Рамальо Антонио, проф. международных отношений, Университет Бразилиа, Бразилиа, Бразилия

Сагер Абдулазиз, основатель и председатель, Исследовательский центр Залива, президент, Sager Group Holding, Дубаи, ОАЭ

Санаи Мехди, доктор политологии, руководитель, Центр по изучению России, Центральной Азии и Кавказа, Тегеран, Иран

Сатановский Евгений Янович, к.э.н., проф., президент, Институт Ближнего Востока, Москва, Россия

Толипов Фарход Фазилович, к.п.н., директор негосударственного научно-образовательного учреждения *Билим карвони (Караван знаний)*, Ташкент, Узбекистан

Тян Чун-Шэн, профессор, заместитель директора, Китайская ассоциация экономических исследований России и Центральной и Восточной Европы, Пекин, КНР

Унникришнан Нандан, вице-президент, старший научный сотрудник Центра по международным вопросам, Фонд *Observer*, Дели, Индия

Эггерт Константин фон, политический обозреватель, радио *КоммерсантЪ FM*, Москва, Россия