Библиотека ПИР-Центра

Олег Демидов

Глобальное управление Интернетом и безопасность в сфере использования ИКТ

Ключевые вызовы для мирового сообщества

Москва
2016

УДК 004.056
ББК 32.971.353
Д30

Редактор А. Куликова

Рецензенты: М. Медриш, А. Федоров, М. Якушев

Демидов О.

Д30 Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества / Олег Демидов. — М.: Альпина Паблишер, 2016. — 198 с. — (Библиотека ПИР-Центра).

ISBN 978-5-9614-5820-6

В рамках этого обзорно-аналитического доклада рассматриваются ключевые вызовы международной безопасности в области использования информационно-коммуникационных технологий на глобальном и национальном уровнях, а также интересы и цели международного сообщества, включая государства и другие заинтересованные стороны, в сфере управления Интернетом.

Доклад подготовлен консультантом ПИР-Центра Олегом Демидовым при участии экспертов рабочей группы при Экспертном совете ПИР-Центра — ведущего российского неправительственного научного центра по вопросам глобальной безопасности.

Публикуемые в докладе материалы, суждения и выводы являются исключительно взглядами автора.

УДК 004.056
ББК 32.971.353

ISBN 978-5-9614-5820-6

Оглавление

Автор благодарит Андрея Баклицкого, Елену Волчинскую, Ульяну Зинину, Елену Зиновьеву, Альберта Зульхарнеева, Виталия Каберника, Мадину Касенову, Александру Куликову, Ирину Левову, Алексея Лукацкого, Михаила Медриша, Алёну Махукову, Владимира Орлова, Наталью Пискунову, Андрея Романова, Илью Сачкова, Максима Симоненко, Екатерину Сизикову, Леонида Тодорова, Александра Федорова, Елену Черненко, Михаила Якушева, Андрея Ярных.

Интернет представляет собой первое изобретение, которое люди создали, но не до конца понимают, крупнейший анархистский эксперимент, на который человечество когда-либо отваживалось.

Эрик Шмидт,
председатель совета директоров Google Inc.

Информационно-коммуникационные технологии (ИКТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI в. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. ИТ быстро становятся жизненно важным стимулом развития мировой экономики. Они также дают возможность всем частным лицам, фирмам и сообществам, занимающимся предпринимательской деятельностью, более эффективно и творчески решать экономические и социальные проблемы. Перед всеми нами открываются огромные возможности.

Окинавская хартия глобального
информационного общества, 2000 г.

Мы вновь подтверждаем провозглашенные во время Женевского этапа ВВУИО в декабре 2003 г. принципы, согласно которым Интернет превратился в общедоступный глобальный инструмент, и управление его использованием должно стать одним из основных вопросов повестки дня информационного общества. Организация использования Интернета на международном уровне должна иметь многосторонний, прозрачный и демократический характер при полном участии правительств, частного сектора, гражданского общества и международных организаций. Она должна гарантировать справедливое распределение ресурсов, облегчать доступ для всех и обеспечивать стабильное и безопасное функционирование Интернета с учетом многоязычия.

Тунисская программа информационного общества
от 15.11.2005 г., параграф 29

ИКТ являются технологиями двойного назначения, которые могут использоваться как в законных, так и в злонамеренных целях. Любое устройство ИКТ может стать источником или объектом злонамеренных действий. Злонамеренное использование ИКТ легко скрыть, а выявление конкретного злоумышленника может быть сопряжено с трудностями, в связи с чем злоумышленники, которые нередко действуют в условиях безнаказанности, могут осуществлять все более сложные вредоносные действия. Эту проблему также усугубляет глобальный охват сетей ИКТ. Глобальный доступ, уязвимые технологии и фактор анонимности облегчают использование ИКТ в целях осуществления подрывной деятельности.

Доклад Группы правительственных экспертов ООН
по достижениям в сфере информатизации
и телекоммуникаций в контексте международной безопасности.
Принят резолюцией Генеральной Ассамблеи ООН A/68/150
от 30.07.2013 г.

Раздел I

Информационно-коммуникационные технологии: критический фактор глобального развития

Глобальные тенденции развития ИКТ

На сегодняшний день информационно-коммуникационные технологии (ИКТ) стали одной из наиболее распространенных, стержневых, в подлинном смысле слова глобальных технологий, определяющих динамику развития мировой экономики и отдельных зависимых от нее ниш и сегментов.

Безусловно, центральной составляющей глобальной ИКТ-отрасли является Интернет. По данным Международного союза электросвязи (МСЭ), к концу 2014 г. количество интернет-пользователей в мире достигло 3 млрд человек, или около 40% населения планеты. Проникновение Сети по миру демонстрирует темпы роста, беспрецедентные для любой другой массовой пользовательской технологии в истории человечества. Только в развивающихся странах за 2009–2014 гг. количество интернет-пользователей выросло вдвое — с 974 млн до 1,9 млрд человек.

Согласно прогнозам к 2017 г. доступ в Сеть будет иметь половина населения Земли (3,5 млрд человек). К 2020 г., по оценкам экспертов Организации по безопасности и сотрудничеству в Европе (ОБСЕ), показатель вырастет до 5 млрд человек. Спустя еще десятилетие уровень проникновения Интернета в развитых странах вплотную приблизится к 100%. Использование Глобальной сети станет повседневной нормой практических для всех демографических групп и социальных страт, включая детей, пенсионеров и малоимущих.

Совокупность рынков и транзакций, определяемая в англоязычной практике как «цифровая экономика» (*Digital economy*), измеряется многими триллионами долларов США, представляя собой самый быстрорастущий столп глобальной экономики. По ряду оценок (компании IDC, IDate), ее совокупный объем, складывающийся из транзакций на рынке электронной коммерции (сегменты «бизнес — бизнесу» и «бизнес — конечным пользователям»), а также рынка цифровых товаров и услуг в 2013 г. составил

2015 г.

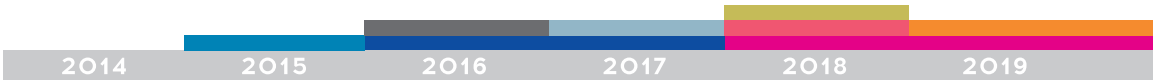
Создание в рамках всемирного Форума по управлению Интернетом (IGF) постоянного Исполнительного секретариата и рабочей площадки по подготовке глобального Договора/Конвенции о ключевых принципах управления Интернетом в горизонте двух–четырех лет.

2016 г.

Разработка и *принятие в формате рекомендательного документа ООН единообразного перечня критической терминологии* в сфере ИКТ и их использования в области международной безопасности с учетом наработок ОБСЕ, ГПЭ ООН и других международных форматов.

2016–2017 гг.

Первый прецедент человеческих жертв в результате промышленного/военного акта саботажа с использованием ИКТ в отношении объектов критической информационной инфраструктуры.



2018–2020 гг.

Приостановка позитивных макроэкономических тенденций в глобальном интернет-секторе вследствие нарастающей политически обусловленной фрагментации Сети по национальным сегментам.

2019–2020 гг.

1. Применение государством кинетических вооружений в ответ на недружественные действия с использованием ИКТ.
2. Эрозия глобальной финансовой системы вследствие развития нерегулируемого рынка криптовалют.

2021 г.

1. Составление международного *единообразного перечня видов объектов КИИ и системы критериев их классификации* с целью использования для развития форматов мер доверия в сфере использования ИКТ.
2. Разработка *рамочного международного соглашения об обеспечении безопасности КИИ в атомной отрасли* (возможно, на площадке МАГАТЭ).

2021 г.

Согласование и принятие глобального юридически обязательного *международного документа (Договора/Конвенции) по борьбе с трансграничной киберпреступностью и кибертерроризмом*, включающего механизмы обмена данными, и задействующего потенциал координационных центров, ассоциаций и альянсов CERT.

Рис. 1. Карта угроз и целей в области использования ИКТ до 2025 г.

2017 г.

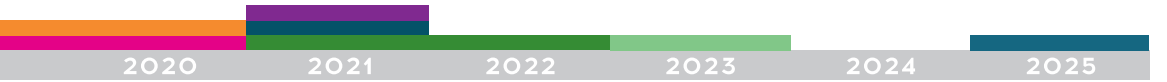
Завершение передачи контроля над критическими функциями Интернета (функции IANA) от правительства США независимой международной структуре, сформированной с участием всех заинтересованных сторон, включая представителей государств.

2018 г.

Принятие разработанного в рамках рабочей площадки Форума по управлению Интернетом (IGF) глобального соглашения о ключевых принципах управления Интернетом в формате Договора/Конвенции ООН.

2018 г.

Формирование в рамках механизмов ООН глобальной диалоговой и координирующей площадки для обсуждения вопросов, выработки политики и норм поведения, а также разработки принятия международных документов с целью том числе предотвращения угроз международной безопасности в области ИКТ и их использования (*Глобальный форум по противодействию ИКТ-угрозам*).



2021–2022 гг.

Принятие на вооружение и использование в международных конфликтах БАРС с летальным вооружением.

2023 г.

Выработка на площадке ООН *согласованного подхода к применению норм существующего международного права (включая нормы международного гуманитарного права и права вооруженного конфликта) в сфере использования ИКТ*. Дополнение Статьи 3 резолюции ГА ООН № 3314 от 14.12.1974 «Об определении агрессии» определением агрессии с использованием ИКТ.

2025 г.

Рассмотрение вопроса о *расширении компетенции Международного уголовного суда* на действия с использованием ИКТ, подпадающие под понятия агрессии, военных преступлений и проч.

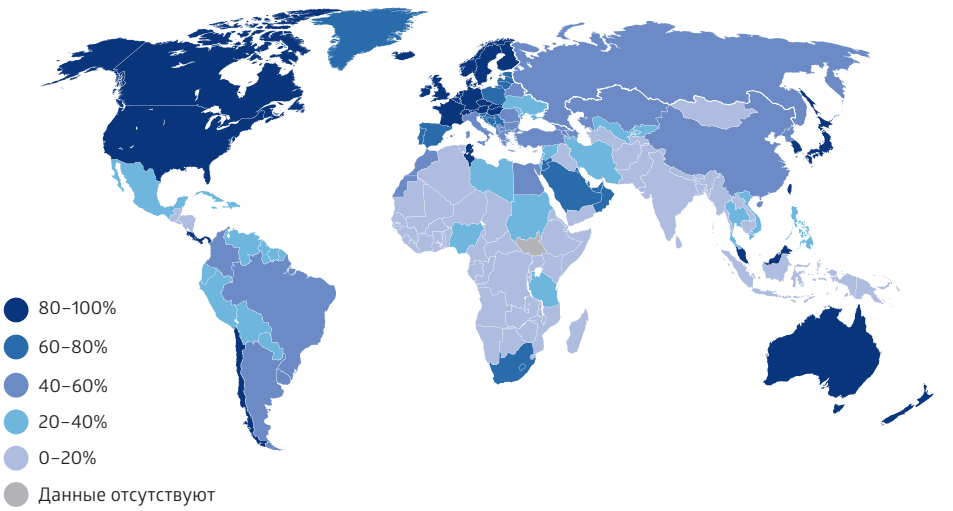


Рис. 2. Уровень проникновения Интернета в мире на 2012 г.

Источник: Internet Society

20,4 трлн долл. США. Для сравнения: эта цифра превышает ВВП США — ведущей экономики мира (15,685 трлн долл. США в 2013 г.) и условно эквивалентна 27,57% глобального валового внутреннего продукта за тот же год.

Масштабы и интенсивность глобального информационного обмена, основанного на Интернете и других сетях, продолжают расти с колоссальной скоростью. В 2012 г. человечество передало в Сеть 44 экзабайта данных — больше, чем за всю свою прежнюю историю. В конце 2013 г. только суммарный объем мобильного интернет-трафика составил 1,5 экзабайт. По прогнозам Cisco Systems, уже в 2016 г. общий объем интернет-трафика превысит 1,4 зетабайта (1,4 трлн Гб), причем более 95% его составит видеотрафик.

«Информационному взрыву» сопутствует стремительное развитие глобальной облачной инфраструктуры. Облачные вычисления (англ. *Cloud Computing*) — совокупность сервисов и решений, основанных на принципе «доступ по требованию» к общему пулу распределенных ресурсов. Исходная концепция была во многом сформулирована в 2005 г. в рамках проекта Amazon EC2, однако «выстрелила» в глобальном масштабе лишь в начале нынешнего десятилетия. Свойства облачных сервисов включают самообслуживание по требованию, объединение ресурсов, универсальный

доступ по Сети, эластичность, а также учет потребления. Успешное освоение этих возможностей различными отраслями экономики ведет к формированию глобального рынка публичных облачных сервисов, объем которого по итогам 2016 г. может вырасти до 204 млрд долл. США. Прогнозируется, что к 2020 г. до 30% всех данных всех данных будет либо храниться, либо передаваться в облаках. Однако наряду с новыми возможностями работы с данными облака генерируют и новые риски информационной безопасности. Наиболее существенным из них является рост уязвимости глобальных облачных хранилищ и зависимости от них как отдельных пользователей, хранящих *в облаке* огромный объем персональных данных, так и бизнеса, использующего *облака* для оптимизации и развития своих критических процессов.

Другие *большие идеи*, такие как Интернет вещей (англ. *the Internet of Things*), наряду с прорывными точками роста ИКТ-сектора также ставят вызовы перед архитектурой Глобальной сети, заставляют ее расширять свои «размеры» и адаптироваться к подключению устройств, количество которых многократно превышает численность человечества[1].

Кроме того, в настоящее время частные компании, структуры гражданского общества и технического сообщества, зачастую при поддержке государств, ведут разработку и реализацию целого ряда проектов и технологий, максимально расширяющих доступ к Интернету и беспроводным сетевым коммуникациям, а также несоизмеримо повышающих их доступность для развивающихся стран. К числу таких проектов относятся:

- фонд Internet.org, созданный Facebook с целью подключения к Сети 5 млрд человек по всему миру, и инициативы Facebook и Google по созданию спутниковых систем, систем околоорбитальных БПЛА и аэростатов, обеспечивающих возможность доступа к Сети в труднодоступных и удаленных районах;
- проекты сверхбыстрого Интернета со скоростью передачи данных от 2 Гб/сек до 10 Гб/сек (Google Fiber) и даже до 1,4 Тб/сек (BT Group) и более; данные технические решения, в частности, реализуются в рамках таких проектов, как Global Environment for Networking Innovations (GENI), а также Internet 2.

---

[1] Более подробно об Интернете вещей см. раздел V «Глобальное управление Интернетом: международно-правовые и международно-политические аспекты».

- проекты создания сетей обмена данными на основе дополняющих или альтернативных нынешнему Интернету технологических решений (сети с ячеистой топологией (Mesh Networks), технологии P2P и т. п.).

Еще более революционные идеи и решения реализуются на стыке интернет-сектора и других отраслей экономики, таких как производство и массмедиа.

Одним из примеров является развитие рынка сервисов и устройств на основе технологии дополненной реальности (англ. *Augmented Reality*), которое включает такие ниши, как визуальный поиск, распознавание информации, визуализация продукции и т. д. Приложениям дополненной реальности прогнозируют уровень проникновения на рынке, близкий к 100% к 2021 г. Причем объем этого рынка уже в 2016 г. может составить порядка 5,15 млрд долл. США, в том числе 209 млн долл. США в российском сегменте.

Еще более грандиозные перспективы открывает технология трехмерной печати (англ. *3D Printing*), рынок которой к 2018 г. может составлять до 2,99 млрд долл. США. Несмотря на относительно скромную оценку емкости рынка, 3D-печать обладает практически универсальным потенциалом в различных сегментах производства. В числе наиболее перспективных отраслей для внедрения технологий 3D-печати называют ВПК (производство оружия и обмундирования, узлов и запчастей для боевой техники, боеприпасов, роботов), биотехнологии (печать искусственных тканей), строительство и инженерное дело — т. е. спектр почти не ограничен. При этом уже сегодня методы 3D-печати, пока несовершенные, позволяют добиться экономии в 97% по финансовым затратам и 83% по времени при производстве таких объектов, как турбовинтовой двигатель (результат достигнут уже в 2011 г.).

Но самое революционное изменение, которое обещает 3D-печать в сочетании с развитием соответствующей ниши программного обеспечения и Интернета вещей — преобразование всей нынешней модели промышленного производства путем ее децентрализации и индивидуализации. По прогнозам Gartner, уже в 2016 г. средняя цена 3D-принтера упадает ниже 2000 долл. США, что сделает эту технику доступной для миллионов индивидуальных пользователей в развитых странах. К этому же времени развитие рынка ПО и виртуальных 3D-моделей, а также совершенствова-

ние самой технологии печати и расширение спектра используемых 3D-принтерами материалов позволят в домашних условиях производить значительную часть всех бытовых товаров и изделий. Несмотря на то что предприятия осваивают 3D-печать раньше конечных пользователей, рост индивидуальной продукции заложен в самом факте развития рынка изменяемых программными средствами виртуальных шаблонов продукции.

Разумеется, и 3D-печать имеет обратную сторону и порождает новые вызовы безопасности. В 2013 г. был напечатан первый функционирующий пистолет, в 2014 г. успешно печатались штурмовые винтовки, запаса прочности которых уже хватает на отстрел нескольких обойм. Потенциальный импульс получает рынок подпольного кустарного производства оружия уже на новом витке технологии. Его регулирование пока относится к числу вызовов ближайшего будущего (по крайней мере, для России), но запас времени здесь крайне ограничен. Необходимо, с одной стороны, активно осваивать эту нишу самим, в том числе в интересах безопасности; а с другой стороны — запускать экспертную проработку возможных последствий развития 3D-печати для мирового рынка вооружений, биотехники, а также сферы организованной преступности и черного рынка. Пока в России имела место одна заметная инициатива — тендер Минобороны на создание биоинженерной печени (шифр «Прометей»), объявленный 20 февраля 2013 г. и завершившийся безрезультатно 15 марта того же года. В настоящее время над проектами сходной направленности ведет работы Фонд перспективных технологий.

В результате реализации этих и других инициатив Интернет наряду с другими сетями продолжит расширять свой пространственный и географический охват. С развитием беспроводной связи пятого, шестого и последующих поколений географическое покрытие беспроводных сетей, их доступность будут расти, пока в мире практически не останется территорий, не покрытых ими. Уже в пределах 10–15 лет стоит ждать повсеместного распространения беспроводных сетей на любой освоенной человеком высоте, глубине, в сложных условиях рельефа, а также, в ограниченной степени, в межпланетном пространстве.

Таким образом, складываются социально-экономические предпосылки для фактического перехода интернет-коммуникации в статус универсального общественного блага (англ. *common good*).

Перспективы права на доступ к Интернету

Повсеместная, почти абсолютная распространенность Интернета в ближайшем будущем вкупе с его огромным значением в хозяйственных, экономических, социальных и собственно коммуникативных процессах как на уровне государств и корпораций, так и на уровне отдельных граждан подтолкнет формирование запроса на включение доступа к цифровым коммуникациям в список базовых прав человека.

Эта тенденция уже обозначила себя и на уровне международных организаций, и в рамках отдельных государств (см. табл. 1).

Развитие данной тенденции не несет в себе особых противоречий и не создает точек напряжения. Более того, бóльшую актуальность она представляет для развитых стран с уровнем проникновения Интернета, приближающимся к 90%, в то время как для России и тем более развивающихся стран, где проникновение не всегда достигает 50%, запрос на такое право пока менее актуален.

Вместе с тем учитывать его все-таки необходимо в контексте выработки политик государственного регулирования интернет-сектора. И в отсутствие кодификации права на доступ в международных документах и закрепления этого права в национальном законодательстве восприятие Интернета как одного из базовых общественных благ обусловливает необходимость поддержания максимально стабильного доступа к Сети. Отключение доступа к Интернету в масштабах региона и тем более государства переходят в глазах граждан в разряд острого кризисного явления.

Яркой иллюстрацией последствий таких ситуаций является эпизод событий так называемой арабской весны в Египте 27–28 января 2011 г., когда крупнейшие египетские интернет-провайдеры одновременно прекратили работу, оставив без доступа в Интернет 93% всех сетей в стране. Результатом действий, приписываемых правительству Мубарака, стал резкий рост интенсивности протестов и числа их участников, возмущенных «информационной блокадой».

Уходя в сторону от столь радикального примера, все же необходимо отметить нежелательность включения в национальное законодательство положений, предполагающих масштабное и/или долгосрочное ограничение доступа в Сеть для большого количе-

Таблица 1. Закрепление права на доступ к Интернету в мире

№	Структура/ государство	Нормы и рекомендации
1	**ООН**	61. В Докладе Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка ла Ру (Frank La Rue) A/66/290 от 10.08.2011 г. отмечается, что «...государства обязаны содействовать осуществлению права на свободное выражение мнений и использованию необходимых для его осуществления средств, к числу которых относится Интернет, или облегчать осуществление такого права и использование таких средств»
2	**ОБСЕ**	В отчете «Свобода выражения мнения в Интернете» представителя по вопросам свободы СМИ Дуньи Миятович (Dunja Mijatovic) 2011 г. утверждается, что «каждый человек имеет право участвовать в жизни информационного общества, поэтому государства обязаны гарантировать доступ граждан к Интернету»
3	**Финляндия**	С июля 2010 г., в соответствии с разделом 60 (3) «Положения об универсальной услуге» (Закон «О рынке коммуникаций» 29), все граждане имеют законное право на доступ к широкополосному соединению со скоростью не менее 1 Мб/сек
4	**Бразилия**	23 апреля 2014 г. был подписан Закон Федеративной Республики Бразилия о порядке использования Интернета № 12.965, известный как Marco Civil da Internet, ставший одним из передовых актов подобного рода в мировой практике. Закон устанавливает принципы, гарантии, права и обязанности использования Интернета в Бразилии. В частности, согласно параграфу I статьи 4 Marco Civil, «Порядок использования Интернета в Бразилии направлен на содействие реализации права каждого на доступ к Интернету». Также, согласно статье 7 закона, «Доступ к Интернету имеет первостепенное значение для осуществления прав и обязанностей гражданина, и пользователям гарантируются следующие права: <...> — IV — право на невозможность приостановки интернет-соединения, за исключением случаев задолженности, ставшей непосредственным следствием использования Интернета; — V — право на обеспечение уровня качества интернет-соединения, предусмотренного договором с провайдером»

ства пользователей. Степень зависимости от Интернета в плане получения информации и участия в коммуникации для граждан такова, что даже в кризисной ситуации подобных мер необходимо избегать любой ценой; данное обстоятельство, в частности, рекомендуется учитывать при выработке стратегии действий в кризисных ситуациях (чрезвычайное положение и т. п.).

Одновременно упрочнение статуса Интернета в перечне базовых общественных благ может способствовать привлечению дополнительного внимания и ресурсов к обеспечению стабильности работы Глобальной сети, а также обеспечению безопасности ее критической инфраструктуры.

Криптовалюты: вызовы и возможности для мировой финансовой системы

Одновременно ИКТ и Интернет создают принципиально новые технологические и инфраструктурные возможности для глобальной финансово-экономической системы. Не имеющими в истории аналогов инструментами ликвидности стали криптовалюты, суммарная капитализация (объем предложения) которых на сентябрь 2014 г. составляла порядка 7 млрд долл. США (из этой суммы более 90% — Bitcoin) и продолжала активно расти. В правовом смысле криптовалюты, основанные на технологии *блокчейна* и представляющие собой распределенные пиринговые платежные системы, являются «*белым пятном*» для финансовой системы, национальных и международных финансовых регуляторов.

Анонимность транзакций и почти неограниченный круг эмитентов делают криптовалюты весьма гибким и удобным платежным средством. Кроме того, отсутствие привязки к каким-либо иным инструментам ликвидности и валютным стандартам, идеальная делимость и мобильность, а также естественный барьер против инфляции, заложенный в сам принцип эмиссии, дают криптовалютам ряд параметров, которые остро востребованы сегодня в контексте реформирования глобальной финансовой системы. По сути, криптовалюты в большей степени подходят под роль средства «отвязки» глобальной финансовой архитектуры от долларового стандарта, чем любое другое существующее современное платежное средство.

Вместе с тем на данном этапе рассматривать криптовалюты в качестве серьезной альтернативы существующим платежным

инструментам не приходится — в силу тех же самых качеств, но с учетом их негативных последствий. Анонимность транзакций делает криптовалюты привлекательным средством для нелегальной торговли, включая торговлю запрещенными товарами и услугами, а также финансирования преступной и даже террористической деятельности.

Виртуальные валюты представляют собой очень интересный международный эксперимент, который ломает парадигму валютной эмиссии. Их определенно не нужно запрещать, их следует пытаться осознать и, может быть, правильно регулировать.

Герман Греф,
президент, председатель правления Сбербанка

С 2011 по 2014 г. наиболее известная криптовалюта Bitcoin использовалась в качестве платежного средства в рамках крупнейших анонимных торговых интернет-площадок Silk Road (*Шелковый путь*), Silk Road 2.0 (*Шелковый путь 2.0*) и других ресурсов, доступных в Сети при использовании специфического программного обеспечения — анонимной сети TOR (англ. *The Onion Router*). Ежемесячный оборот сети на пике ее активности в 2012–2013 гг. за счет торговли оружием, наркотиками и иными запрещенными товарами составлял до 14–15 млн долл. США ежегодно в стоимостном эквиваленте Bitcoin. За время работы ресурса в 2011–2013 гг. суммарный оборот превысил 9,5 млн биткоинов (1,2 млрд долл. США), включая более 600 000 биткоинов, выплаченных в качестве комиссий самой площадке по ставке от 8 до 15% за транзакцию. По данным российской компании Group-IB, криптовалюты, включая Bitcoin, с 2012–2013 гг. также стали одним из распространенных средств расчета при оказании услуг на российском рынке киберпреступности (аренда ботнетов, продажа баз персональных данных и т. д.).

В настоящее время большинство государств мира, включая страны ЕС, США, Сингапур и другие государства Юго-Восточной Азии, идут по пути постепенной легализации оборота, обмена и иного использования криптовалют. Как минимум 28 государств и территорий к началу 2015 г. признали возможность ведения деятельности с использованием криптовалют на своей территории.

Вместе с тем некоторые страны, в том числе Китай и Россия, пытаются проводить политику ограничения использования криптовалют в качестве платежного средства или иного вида легальных активов. Некоторые государства и территории (КНР, Тайвань и Исландия) существенно ограничили оборот криптовалют, но не ввели полного запрета. К марту 2015 г. лишь шесть государств полностью запретили оборот криптовалют: Бангладеш, Боливия, Эквадор, Кыргызстан, Таиланд и Вьетнам. Однако до сих пор законодательные запреты в отдельных странах и юрисдикциях слабо влияют на размер эмиссии, объем оборота и спрос на эти инструменты. С момента ареста основателя Silk Road в 2013 г. до последнего квартала 2014 г. курс Bitcoin вырос в четыре раза; по состоянию на ноябрь 2015 г. он удерживался в коридоре 300–400 долл. США/1 BTC.

В международных структурах выработка позиций по работе с криптовалютами в целом идет медленнее, чем на страновом уровне. Ни Всемирный банк, ни Международный валютный фонд по состоянию на июнь 2015 г. не выработали целевых рекомендаций по криптовалютам. Наиболее активную позицию по поводу криптовалют пока занимает упомянутая выше ФАТФ со своим списком рекомендаций, изложенным в докладе от 15 июня 2015 г. Появление первой межгосударственной политики регулирования криптовалют также возможно на площадке ФАТФ — в июне 2015 г. три ведущие экономики мира, США, КНР и Япония обратились в Группу с проектом общей концепции, направленной на предотвращение рисков в сфере ОД/ФТ, связанных с использованием криптовалют. В случае одобрения концепции появится шанс на ее принятие всеми странами — членами ФАТФ и появление первого в своем роде режима регулирования криптовалют.

В отсутствие эффективного регулирования криптовалют запреты окончательно вытеснят их на черный рынок, что лишь усилит финансовую подпитку криминала, а также создаст угрозу всей глобальной финансовой системе в случае, если переток средств между ее легальным и теневым виртуальным сегментами достигнет достаточных объемов.

В этой связи необходимо учитывать, что уже сейчас пиринговые распределенные платежные системы на основе блокчейна за счет стран с либеральным подходом к их регулированию превращаются в подрывную инновацию на глобальном рынке финансовых ус-

луг и инструментов. Магистральная тенденция в США — расширение круга крупных ИТ-компаний, принимающих криптовалюты к оплате. В июле 2014 г. крупнейшей корпорацией, принимающей к оплате биткоины, стал ИТ-гигант Dell. С сентября 2014 г. платежи в биткоинах на территории США начал принимать PayPal. В декабре 2014 г. оплата в биткоинах стала доступна для американских клиентов в ряде онлайн-магазинов корпорации Microsoft (Windows, Windows Phone, Xbox Games, Xbox Music и Xbox Video). Принимать к оплате биткоин в 2014 г. начали и некоторые крупные американские ретейлеры, включая Overstock и Newegg. Дальнейшее развитие этого тренда и распространение его на глобальный рынок финансовых услуг может привести к доминирующей роли криптовалютных платежных систем в этой рыночной нише.

Вместе с тем сама технология блокчейна, распределенной криптографически заверенной и защищенной цепочки, системы записи транзакций, предлагает еще более фундаментальные инновации, чем сами криптовалюты, во множестве ниш от международных межбанковских расчетов до развития глобальной индустрии Интернета вещей. Отметим лишь следующие факты:

- Весной 2015 г. Банк Англии опубликовал аналитическую записку, в которой в том числе оцениваются теоретические перспективы эмиссии собственных криптовалют национальными центральными банками. При этом упоминаются возможности ввода в оборот аналога обычной валюты, доступной как банкам, так и неограниченно широкому кругу субъектов, включая физических лиц.
- Также регулятором была описана теоретическая возможность использования технологии блокчейна для создания системы межбанковских расчетов нового поколения. По сути, речь может идти о создании альтернативы глобальной системе межбанковских расчетов SWIFT, часто критикуемой за технологический консерватизм и использование устаревших решений и протоколов.
- В январе 2015 г. два высокотехнологичных гиганта — IBM и Samsung опубликовали предварительное техническое описание проекта на базе блокчейна и пиринговых протоколов, нацеленного на продвижение услуг и решений на рынке Интернета вещей (IoT). Концепция новой технологической платформы — ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry) —

основана на интеграции трех программных решений: TeleHash, децентрализованного пирингового (P2P) протокола для обмена данными и передачи сообщений; BitTorrent, пирингового сетевого протокола для кооперативного обмена файлами; а также Ethereum — виртуальной машины, основанной на блокчейне и наборе сервисов Web 3.0, дающей пользователям возможность работать с программной средой *умных контрактов* (smart contracts), развивая и наполняя ее контентом по своему усмотрению за счет поддержки контрактного программирования. За счет этих решений IBM и Samsung надеются разработать глобальную экосистему умных объектов (прежде всего продукции в нише бытовой электроники), которая полностью поменяет рынок проприетарных корпоративных стандартов Интернета вещей.

Таким образом, фундаментальный инновационный и экономический потенциал технологии блокчейна и основанных на ней продуктов, включая криптовалюты, выглядит бесспорным. Вместе с тем бурное развитие таких продуктов и технологий в глобальном масштабе создает вызов для национальных финансовых систем и экономик, где не будет проводиться эффективное регулирование этих инновационных инструментов, их нормативное сопряжение и встраивание в привычные технологии и институциональные рамки финансовых механизмов. Нужно особо подчеркнуть, что сугубо запретительная модель регулирования криптовалют несет в себе высокие риски неэффективности, поскольку современные финансовые потоки и системы преимущественно трансграничны, а значит, трансграничными будут и последствия легализации инноваций на основе блокчейна в любых других странах и юрисдикциях, особенно таких значимых для глобальной финансовой системы, как США и страны ЕС.

Российская повестка дня в отношении интернет-сектора

Россия прочно удерживает и закрепляет статус одного из мировых лидеров в развитии национального интернет-сектора в различных его сегментах:

- занимает 7-е место в мире и 1-е место в Европе по количеству интернет-пользователей;

- входит в топ-5 национальных сегментов Интернета по уровню связности;
- русский язык входит в тройку самых распространенных языков в Сети по количеству ресурсов (5,7% веб-страниц на русском в сентябре 2013 г.);
- с 2000 по 2013 г. число русскоязычных интернет-пользователей выросло в 27,22 раза и достигло 87,48 млн человек на декабрь 2013 г. (7-е место в мире среди всех языков);
- в доменной зоне .ru зарегистрировано 1,8% всех доменов в Сети (4,89 млн), что делает ее пятой по популярности страновой доменной зоной верхнего уровня (ccTLD) и обеспечивает место в десятке крупнейших доменных зон верхнего уровня вообще (как среди gTLD, так и ccTLD);
- Россия — одна из четырех стран мира, где на рынке доминируют «домашние» социальные сети. «ВКонтакте» на 8-м месте в мире среди социальных сетей по размеру уникальной ежемесячной аудитории (порядка 80 млн человек);
- Россия — одна из трех стран мира наряду с КНР и США, где на рынке доминируют «домашние» поисковые системы («Яндекс» занимал 57,4% российского рынка поиска в сентябре 2015 г.);
- Интернет играет критическую роль в поддержании и продвижении русского языка за рубежом; от 73 до 86% сайтов в Белоруссии, Украине, Таджикистане, Казахстане и Киргизии наполняются контентом на русском языке;
- один из крупнейших в Европе интернет-холдингов — российская Mail.Ru Group с капитализацией в 4,01 млрд долл. США (декабрь 2015 г.);
- один из глобальных лидеров в сегменте интернет-безопасности для конечного пользователя — российская «Лаборатория Касперского»: 5,5% мирового рынка антивирусного ПО, 711 млн долл. США выручки в 2014 г., более 300 млн индивидуальных клиентов.

По итогам 2014 г. общий объем экономики интернет-зависимых рынков в России оценивался в 11,8 трлн руб., что составляло порядка 16% от национального ВВП. Этот показатель уже превышает вклад в ВВП таких отраслей, как сельское и лесное хозяйство, охота (3,7% в сумме за 2013 г.) и даже строительный сектор (6,5% за 2013 г.).

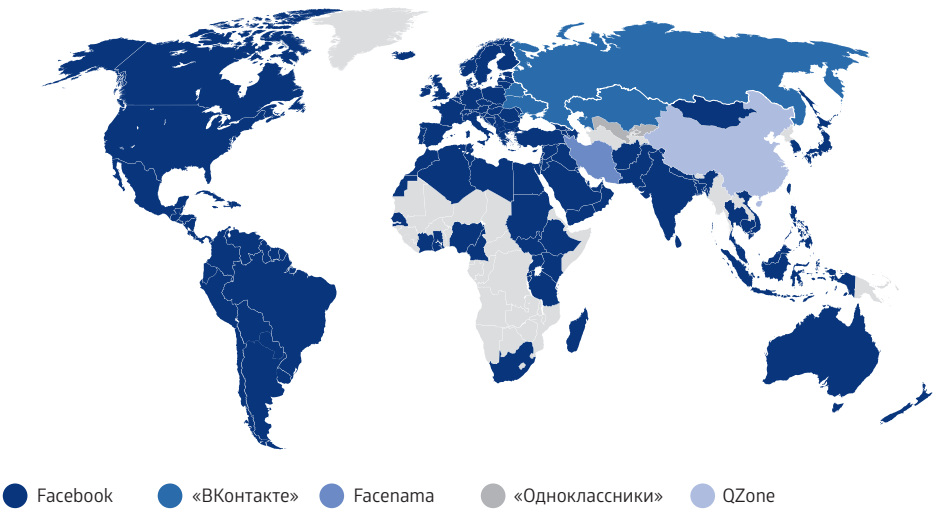


Рис. 3. Преобладающие социальные сети в августе 2014 г.

Источник: VincosBlog

По данным исследования «Экономика Рунета 2014–2015», проведенного Российской ассоциацией электронных коммуникаций (РАЭК) совместно с Национальным исследовательским университетом ВШЭ, объем собственно российских интернет-рынков (контент и сервисы) по итогам 2014 г. составил 1094 млрд руб., а объем рынка электронных платежей — 476 млрд руб., что в сумме эквивалентно 2,2% национального ВВП. При этом по состоянию на лето 2015 г. аудитория Рунета составила 77,5 млн человек старше 18 лет (66% населения), а 62 млн выходили в Интернет каждый день.

Несмотря на прогнозируемое снижение в связи с общей нестабильностью и ухудшением экономической ситуации в стране, даже пересмотренные РАЭК темпы развития интернет-зависимых отраслей несопоставимы с общей динамикой национальной экономики. В исследовании РАЭК и НИУ ВШЭ «Экономика Рунета 2013–2014» при стабилизационном сценарии развития прогнозировался рост российского интернет-сектора и интернет-зависимых отраслей до 2018 г. на уровне 15–20% ежегодно. Даже при негативном сценарии ежегодный рост отрасли до 2018 г. составит 6–10%. В рамках упомянутых сценариев объем экономики Рунета к 2018 г. может

составить до 1872 млрд руб., а объем интернет-зависимых рынков — вырасти до 14,29 трлн руб.

Для сравнения: среднегодовые темпы роста российской экономики в целом, согласно Прогнозу долгосрочного социально-экономического развития РФ на период до 2030 г., подготовленному Министерством экономического развития РФ, в 2013–2030 гг. составят всего порядка 3%.

Таким образом, ИКТ, и, в частности, интернет-зависимые сектора экономики, стали одним из ведущих несырьевых моторов российского экономического роста и инновационного развития. Названные отрасли имеют все шансы удержать за собой эту функцию и в течение как минимум ближайшего десятилетия при условии стабилизации экономической ситуации, грамотного регулирования со стороны государственных ведомств, в том числе с учетом реализации долгосрочной стратегии по импортозамещению в сфере ИТ. Большое значение также имеет дальнейшее развитие внешнеполитической ситуации, в частности преодоление конфронтации с западными партнерами.

В этих условиях всесторонняя государственная поддержка и режим максимального благоприятствования, создания положительных стимулов и точек роста для ИКТ-сектора могут рассматриваться в качестве потенциальных ключевых приоритетов как кратко-, так и среднесрочной, а также долгосрочной стратегии развития отечественной экономики.

Также актуальными видятся следующие выводы и предложения.

1. Интернет-отрасль могла бы быть признана одним из ключевых секторов экономики Российской Федерации и отражена в этом качестве в стратегических документах и законодательстве.

Отдельные объекты и информационные системы российского сегмента Сети могут быть признаны объектами критической инфраструктуры вне зависимости от того, в какой форме собственности они находятся. В этом случае для государства целесообразно обеспечить надлежащий уровень безопасности таких объектов и максимальную стабильность их функционирования. В качестве примера можно упомянуть инфраструктуру, обеспечивающую работу сервисов «Яндекса» на территории России, которыми ежедневно пользуются миллионы российских граждан для получения информации и организации своих бизнес-процессов.

2. Целесообразным шагом могло бы стать адекватное и достаточное отражение ключевой роли Интернета в развитии российской экономики на уровне системы органов государственной власти, отвечающих за стимулирование и поддержку данной отрасли. Институциональная инфраструктура управления интернет-отраслью, адекватная роли Интернета в развитии российской экономики, должна включать ответственный орган, координирующий орган, систему органов (должностных лиц, включая президента) для выработки стратегических международных и внутриполитических решений. На сегодняшний день функции и компетенции, связанные с развитием интернет-отрасли, преимущественно закреплены за Министерством связи и массовых коммуникаций РФ, однако не все аспекты интернет-отрасли находятся в компетенции ведомства.

Полезен может быть постоянный тесный диалог по всему спектру вопросов безопасности, связанных с интернет-сектором, начиная с вопросов безопасности контента, заканчивая обеспечением стабильности работы критической инфраструктуры Рунета. Со стороны государства механизмом для ведения такого диалога могла бы стать межведомственная координационная площадка, включающая сотрудников МИД РФ, Министерства связи и массовых коммуникаций РФ, ФСБ РФ, МВД РФ, Роскомнадзора, Министерства экономического развития и проч.

Своевременным и назревшим решением представляется учреждение в феврале 2014 г. поста Специального представителя президента России по вопросам международного сотрудничества в области информационной безопасности, который в настоящее время занимает опытный дипломат, один из главных архитекторов российской внешнеполитической линии по вопросам информационной безопасности А.В. Крутских. Востребовано также оказалось создание поста общественного омбудсмена по вопросам развития интернет-отрасли, подчиняющейся непосредственно российскому бизнес-омбудсмену. В июле 2014 г. на пост интернет-омбудсмена был назначен российский предприниматель в сфере ИТ Д.Н. Маричев. В декабре 2015 г. для решения вопросов развития и регулирования Интернета в России был впервые учрежден пост в структуре Администрации президента РФ. Первым советником президента по вопросам развития Интернета стал известный представитель российской интернет-отрасли Г.С. Клименко. Безусловно, закреп-

ление повестки дня развития и регулирования Рунета на столь высоком уровне властной иерархии — знак растущего внимания государства к проблемам и возможностям этой отрасли. Однако в такой ситуации особенно важен баланс между интересами самого государства как регулятора с одной стороны, частной отрасли Рунета — с другой, и сообщества российских интернет-пользователей — с третьей. Все эти три крупные группы стейкхолдеров имеют свои интересы, зачастую не совпадающие друг с другом, что уже было отмечено в интервью и публичных выступлениях г-ном Клименко. Вопрос в том, как сбалансировать и уравновесить эти интересы и возможности их легального выражения и продвижения, не создавая драматического перекоса в пользу позиций политико-административного аппарата или крупного бизнеса. Нужен ли сообществу российских интернет-пользователей собственный представитель, наделенный полномочиями и имеющий доступ к публичным каналам выражения мнений? В качестве условного прототипа такого коллективного представителя можно рассматривать российское общественно-политическое объединение «Пиратская партия России», во многом защищающее и представляющее интересы рядовых пользователей в дискуссии по вопросам интеллектуальной собственности в Интернете и борьбе с интернет-пиратством на российской рынке цифровой медиапродукции.

3. Одной из возможных приоритетных задач для государства могло бы стать создание необходимых условий для развития российского интернет-бизнеса на внешних рынках, их участия в глобальной конкуренции. Инициативы в сфере государственного регулирования, преследующие цель уменьшения физической связности между российским сегментом и Глобальной сетью, направленные на инфраструктурную либо иную автономизацию, отграничивание Рунета, напротив, могут иметь для отрасли сложнопредсказуемые последствия.

Оставляя за скобками вопросы прав человека, следует подчеркнуть, что рост и экспансия российского интернет-бизнеса в критической степени определяются *эффектом масштаба*, возведенным в глобальную степень в случае с Интернетом. Нивелирование этого эффекта в случае фрагментации Сети и обособления ее российского сегмента может в конечном счете способствовать постепенному истощению резервов его роста по мере насыщения внутреннего рынка.

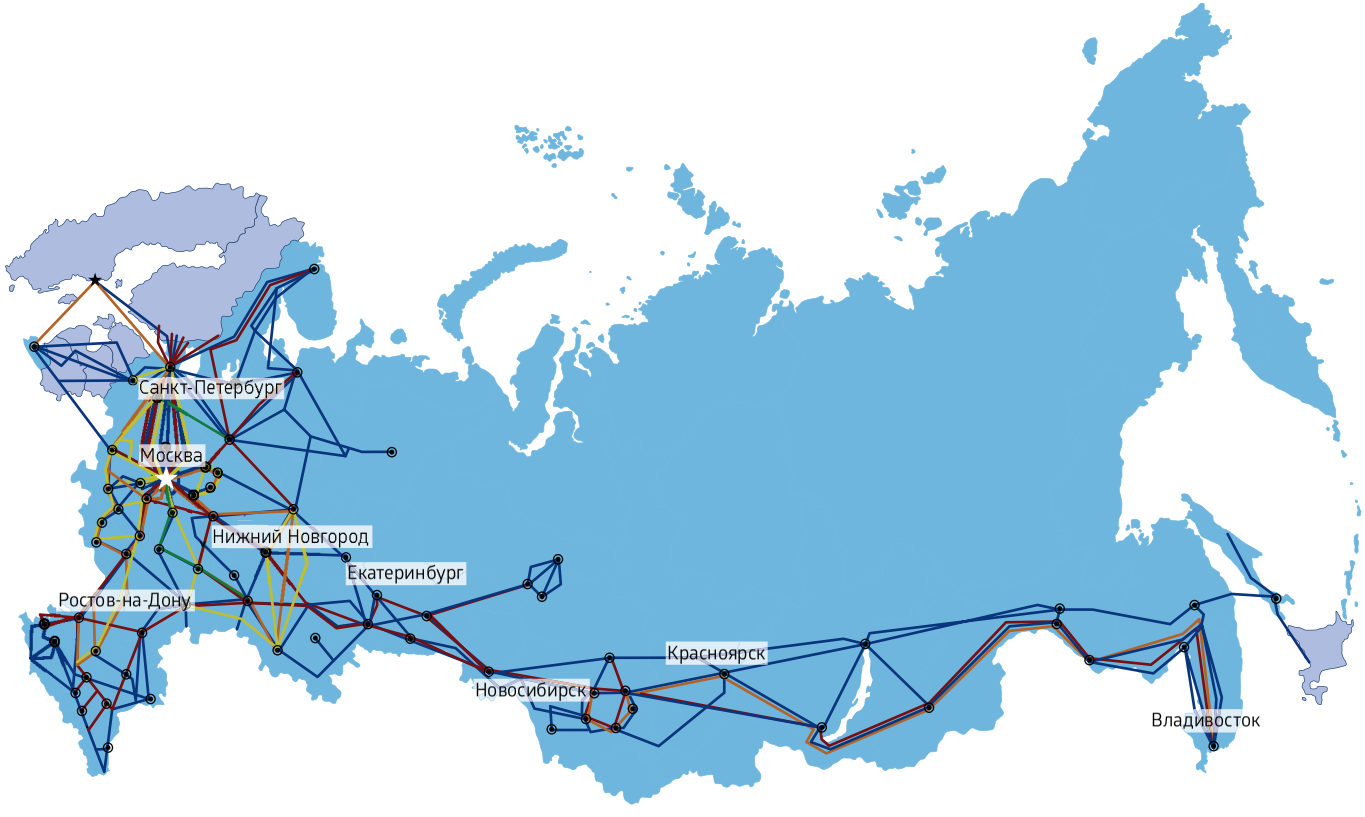


Рис. 4. Магистральные сети российских провайдеров по состоянию на февраль 2014 г.

Источник: Rubroad.ru

4. Целесообразен может быть пересмотр роли и возможностей Рунета в качестве средства продвижения и сохранения российской и русской культурно-языковой идентичности, популяризации и глобализации российского культурного наследия, равно как и современной культуры. Онлайн-инструменты и интернет-проекты, как представляется, могли бы получить приоритетную роль в методологии работы таких структур, как Россотрудничество. Колоссальный потенциал российской интернет-отрасли в этой сфере создает хорошие точки синергии и с внешнеполитическими задачами страны, решением которых занимается МИД. Развитие инструментов «цифровой дипломатии» также видится востребованной и перспективной стратегией, формулировать и осуществлять которую, однако, было бы наиболее эффективно при активном вовлечении самой интернет-отрасли.

5. Своевременной и востребованной видится проактивная стратегия государства в направлении освоения принципиально новых технологических ниш, открывающихся в сфере ИКТ. В частности, речь может идти о стимулировании освоения российской экономикой, и прежде всего частным сектором, оборудования и технологий 3D-печати, поддержка усилий частного сектора, активизация государственного регулирования — но в ключе не ужесточения, а либерализации, — с целью ускоренного развития сегментов рынка. Опережающее реагирование на развитие подобных новых технологий в части их регулирования, во-первых, позволяет купировать генерируемые ими риски и вызовы безопасности, а во-вторых, создает условия для их развития на местном рынке, содействуя их переводу из фактора отставания в асимметричное рыночное преимущество.

Дополнительная информация

1. Рунет сегодня. Аналитика, цифры, факты. Открытие РИФ+КИБ 2014. 23–25 апреля 2014 г. URL: http://tpp.nnov.ru/data/pages/82/files/Internet_segodnya.pdf (дата обращения: 01.03.2016).
2. Экономика Рунета 2013–2014. Организаторы: РАЭК, НИУ ВШЭ. Москва, 2013 г. URL: http://xn--80aaokjbmheeb2a2al4l.xn--p1ai/2015 (дата обращения: 01.03.2016).
3. ICT Facts and Figures. The World in 2014. International Telecommunication Union. URL: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (дата обращения: 01.03.2016).

4. The Global Information Technology Report 2014. Rewards and Risks of Big Data. Insight Report. Beñat Bilbao-Osorio, Soumitra Dutta, and Bruno Lanvin, Editors. World Economic Forum. URL: http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf (дата обращения: 01.03.2016).
5. Демидов О.В. От права на доступ к сетевому разуму. Российский совет по международным делам. 29.03.2013. URL: http://russiancouncil.ru/inner/?id_4=1618#top-content (дата обращения: 01.03.2016).
6. Демидов О.В. Связанные одним блокчейном: обзор международного опыта регулирования криптовалют. Индекс безопасности № 2 (113). Том 21. С. 41–60. URL: http://www.pircenter.org/media/content/files/13/14374603770.pdf (дата обращения: 01.03.2016).

Документы

1. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. Генеральная Ассамблея ООН, A/66/290, 10.08.2011. URL: http://www.un.org/Docs/asp/ws.asp?m=A/66/290 (дата обращения: 01.03.2016).
2. Communications Market Act (393/2003; amendments up to 363/2011 included). Ministry of Transport and Communications, Finland. URL: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030393.pdf (дата обращения: 01.03.2016).
3. Свобода выражения мнения в Интернете. Отчет. Организация по безопасности и сотрудничеству в Европе. 15.12.2011. URL: http://www.osce.org/ru/fom/89063 (дата обращения: 01.03.2016).
4. Касенова М. Авторский перевод Закона об Интернете Федеративной Республики Бразилия (Law No 12.965, Marco Civil Da Internet) // Электронный журнал ПИР-Центра «Пульс кибермира». Январь–февраль 2015 г. № 1 (13). URL: http://pircenter.org/articles/1841-avtorskij-perevod-zakona-ob-internete-federativnoj-respubliki-braziliya-law-no-12965-marco-civil-da-internet (дата обращения: 01.03.2016).

Раздел II

Вопросы безопасности в области развития и применения ИКТ в глобальном контексте:
на пути к единой терминологии и общим подходам

По мере развития государственных политик в области использования ИКТ и управления Интернетом, а также развития международных дискуссий и попыток выработать международные договоренности, нормы и правила в этой сфере, растет значение используемой терминологии и заключенных в ней подходов.

В то же время отмечается усиление противоречий и политизация дискуссии именно вокруг терминологической составляющей предлагаемых доктринальных документов, национального законодательства, а также международных документов и их проектов, прежде всего по вопросам безопасности в области использования ИКТ.

С середины 1990-х гг. в США, а затем в Европе и во многих других странах получила распространение концепция и терминология *кибербезопасности*, опирающаяся прежде всего на понятие *киберпространства* как особой нефизической среды ИКТ. Несмотря на то что эти термины и производные от них понятия далеко не всегда употреблялись в национальных законодательствах разработавших и принявших их государств, а также далеко не всегда получали официальные определения, к настоящему дню терминология и идея кибербезопасности прочно закрепились как в профессиональном сообществе и частном секторе, так и в доктринальных и стратегических документах большого количества стран, надгосударственных образований (Европейский Союз), международных организаций (НАТО, Совет Европы, Региональный форум АСЕАН, ОЭСР, ОБСЕ и проч.).

Практически параллельно в ряде других государств, включая прежде всего Россию, получили развитие альтернативные концепции и подходы, основанные на иной терминологии. Наиболее целостным и системным из их числа можно считать концепцию международной информационной безопасности (МИБ), которая была изначально сформулирована Россией, а затем получила развитие и поддержку среди членов Шанхайской организации

сотрудничества (ШОС), а также других государств и международных форматов (СНГ, ОДКБ).

С момента начала в 1998 г. деятельности по продвижению на международных площадках (прежде всего ООН) своего подхода Россия столкнулась с оппозицией со стороны ряда развитых государств, международных форматов, технического сообщества и зарубежного частного бизнеса. Оппоненты, в том числе эксперты и дипломаты США и стран Западной Европы, отмечали несоответствие российского подхода практикам, сложившимся в международном сообществе технических экспертов, и практикам частного сектора в большинстве стран мира.

Основной причиной стало расхождение двух подходов по поводу того, включается ли такой аспект, как влияние содержания информации на социально-политические и иные общественные процессы, в круг вопросов, подлежащих рассмотрению, согласованию и, в перспективе, международному регулированию в рамках проблематики ИКТ-безопасности. Хотя справедливости ради нужно отметить, что кибербезопасность отнюдь не ограничивается техническими аспектами (например, Европейская конвенция по кибербезопасности включает в качестве вида преступления распространение детского порно).

Содержание информации, генерируемой и передаваемой посредством ИКТ, и ее влияние на общественные процессы является одним из краеугольных камней в рамках МИБ. В то же время в практике США, государств Западной Европы, ряда других стран и международных форматов данный аспект не рассматривается в контексте кибербезопасности и ИКТ вообще. Данные вопросы рассматриваются ими в контексте соблюдения прав и свобод человека (свобода слова, свобода самовыражения), либо в плоскости безопасности исключительно в контексте противодействия терроризму и экстремизму, т. е. вне ИКТ-специфичного контекста. Собственно, в рамках повестки дня кибербезопасности упор делается на обеспечение и поддержание безопасности и стабильной работы ИКТ-инфраструктуры. «Человеческое» и «контентное» измерение проблемы при этом играет также важную, но *опосредованную* роль.

Еще один водораздел двух концепций проходит по вопросу о трактовке государственного суверенитета применительно к сфере ИКТ. Концепция МИБ утверждает незыблемость и верховен-

ство государственного суверенитета в сфере ИКТ и предлагает механизмы достижения договоренностей, основанные прежде всего на межгосударственном взаимодействии. Концепция кибербезопасности как таковая не содержит конкретной позиции по вопросам суверенитета, так как он выпадает за ее рамки. Однако фундаментальное видение процессов в области ИКТ, заключенное в этом подходе, предполагает признание трансграничного характера киберпространства и, соответственно, ограниченной, неполной применимости к нему понятия и практик государственного суверенитета. Отсюда вытекает принципиальное расхождение сторон в вопросе о том, какие механизмы и инструменты регулирования применимы для обеспечения безопасности в сфере ИКТ на уровне государства и на международном уровне.

Конфликт между концепциями МИБ и кибербезопасности прослеживается и на национальном уровне регулирования в России, притом что понимание терминов в рамках кибербезопасности за рубежом также далеко не единообразно (см. табл. 2). Попытка привлечения экспертного сообщества и частного сектора к составлению доктринального документа, предпринятая в 2012–2013 гг. на площадке российского Совета Федерации, показала четкое наличие у этих заинтересованных сторон запроса на отражение в таком документе вопросов кибербезопасности. Результатом стала Концепция стратегии кибербезопасности Российской Федерации, которая многими экспертами оценивается как прогрессивный документ, отражающий мировые тенденции в области использования ИКТ. Вместе с тем разработанный экспертами документ получил немало критических отзывов, в том числе со стороны МИД РФ, а также Совета Безопасности РФ и ФСБ РФ.

Одной из причин стал тот факт, что текст концепции Стратегии явно идет вразрез с терминологией и концепцией предыдущих нормативных актов и доктринальных документов, начиная с Доктрины информационной безопасности Российской Федерации от 2000 г. и заканчивая Основами государственной политики России в области международной информационной безопасности на период до 2020 г., принятыми также в 2013 г. Таким образом, терминологический и концептуальный конфликт по вопросам безопасности в сфере использования ИКТ является уже и внутрироссийской реальностью, что увеличивает значимость задачи по его скорейшему разрешению.

Таблица 2. Определения киберпространства / информационного пространства

№	Термин	Определение	Государство / источник
1	**Киберпространство**	Глобальное пространство в пределах информационной среды, состоящий из взаимозависимой сети инфраструктур информационных технологий, в том числе Интернета, сетей связи, компьютерных систем, встроенных процессоров и контроллеров	Словарь военных и связанных с ними терминов Министерства обороны США, 2012
2	**Киберпространство**	Виртуальное пространство всех ИТ-систем, связанных на уровне данных в глобальном масштабе. Основу киберпространства составляет Интернет как универсальная и общедоступная сеть передачи данных, которая может дополняться и расширяться за счет любого количества сетей данных. ИТ-системы в изолированном виртуальном пространстве не являются частью киберпространства	Стратегия кибербезопасности для Германии, ФМВД, 2011
3	**Информационное пространство**	Сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию	Соглашение между Правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности» от 16.06.2009 г.
4	**Киберпространство**	Сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, а также любых форм осуществляемой с их использованием деятельности, в том числе частными лицами, организациями и государством	Концепция стратегии кибербезопасности Российской Федерации (проект от 10.01.2014 г.)

Расхождение в трактовке государственного суверенитета в области ИКТ также обусловливает разное видение объема компетенций и полномочий государства в отношении ключевого элемента ИКТ-инфраструктуры — Интернета. Основанная на саморегулировании модель работы технического сообщества, которая исторически сложилась в США и утвердилась за их пределами, легла в основу концепции управления Интернетом с участием всех заинтересованных сторон (англ. *multistakeholder internet governance*). Суть ее сводится к тому, что процесс управления Интернетом может осуществляться должным образом лишь при условии равноправного участия в нем представителей всех групп/сторон, которые непосредственно заинтересованы в развитии Глобальной сети. Изначально к таким «заинтересованным сторонам» относили государство, частный сектор и гражданское общество; по мере развития подхода этот список пополнился сообществом интернет-пользователей и техническим сообществом, что опять же не делает его закрытым.

Данный принцип получил признание и был зафиксирован в решениях Тунисского этапа Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) в 2005 г. Практически все страны мира, включая Россию, разделяют и поддерживают решения ВВУИО, как и сам подход с участием всех заинтересованных сторон — что не устраняет расхождений в его прочтении и трактовке. Российская Федерация, как и ряд ее партнеров на международной арене, не считает, что управление с участием всех заинтересованных сторон умаляет полноту государственного суверенитета по вопросам управления Интернетом; следовательно, принятие решений на международной арене в этой области должно осуществляться представителями государств. Прочие заинтересованные стороны должны включаться в процедуры обмена мнениями, консультирования и обсуждения на стадии проработки решений, но не могут самостоятельно принимать их, тем самым подменяя собой государство как единственный источник суверенитета в соответствии с международным правом[1].

Различные подходы и обусловленные ими понятийные системы, как в части безопасности в сфере ИКТ, так и в части управления

[1] Подробно вопросы управления Интернетом с участием всех заинтересованных сторон см. в разделе V «Глобальное управление Интернетом: международно-правовые и международно-политические аспекты».

Интернетом, имеют полное право на сосуществование. Однако в течение последних лет конкуренция концепций и терминологии в этой области развивается в русле политизации проблемы, что зачастую затрудняет и тормозит практическое решение проблем и выработку механизмов взаимодействия между сторонами.

Так, противоречия между США и Россией по терминологическим вопросам в сфере ИКТ-безопасности как минимум на год задержали подписание прорывных двусторонних соглашений, включающих реализацию комплекса мер доверия с целью предотвращения угроз безопасности в сфере использования ИКТ. Пакет из трех соглашений, готовившийся с 2011 г. для подписания президентами США и России на полях саммита G20 в Лос-Кабосе, Мексика, 18–19 июня 2012 г., удалось подписать лишь годом позже, 17 июня 2013 г. В результате перспективы этого формата сотрудничества оказались под вопросом год спустя в свете ухудшения двусторонних отношений России и США, когда еще не все механизмы были отлажены и опробованы на практике. Будь соглашения подписаны парой лет раньше, механизм мог бы иметь бóльшую ценность и устойчивость даже в условиях кризиса двусторонних отношений.

В более широком смысле терминологические конфликты блокируют шансы на конструктивную работу на международных дискуссионных площадках (серия Международных конференций по вопросам киберпространства в Лондоне, начиная с 2011 г.), не позволяя сторонам сконцентрироваться на действительно важных долгосрочных задачах. К числу таких задач можно отнести формирование институционального каркаса для глобальной системы борьбы с ИКТ-угрозами и предупреждения трансграничных конфликтов с использованием ИКТ.

В неменьшей степени терминологические противоречия препятствуют реформе и обновлению системы международного права с целью эффективного международного противодействия угрозам, обусловленным развитием новейших информационных технологий[1].

Отсутствие прогресса в решении этих проблем, обусловленное в ряде случаев неспособностью договориться на уровне термино-

[1] Подробно см. раздел IV «Использование ИКТ в военно-политических целях: вызовы глобальной безопасности и международному праву».

логии, может быть чревато сползанием международной ситуации в полосу затяжных и разрушительных кризисов и конфликтов с использованием ИКТ уже в горизонте пяти–восьми лет.

В этой связи может быть востребована проработка следующих возможностей.

1. Деполитизация терминологических вопросов применительно к сфере ИКТ-безопасности и вывод их за рамки процесса выработки механизмов взаимодействия там, где это возможно. Параллельным шагом могла бы стать активизация работы над консенсусной терминологией на международных площадках.

2. Выделение и согласование в рекомендательном формате перечня терминов, не требующих определения и интерпретации в силу своей универсальности либо де-факто сложившегося единообразного понимания. Возможные площадки: Группа правительственных экспертов (ГПЭ) ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, Организация по безопасности и сотрудничеству в Европе.

Примером такого термина может служить термин «интернет» — изначально название Глобальной информационно-телекоммуникационной сети, на сегодняшний день вошедшее в употребление в качестве *глобальной технологии коммуникации* и даже, как отмечалось выше, *общественного блага*. Прецедент определения понятия «интернет» был задан в 2004–2005 гг. Эксперты Рабочей группы при Генеральном Секретаре ООН пришли к выводу о том, что данное понятие не нуждается в официальных пояснениях и определениях именно в силу своей очевидности и универсального понимания.

3. Уход от терминологического конфликта «кибербезопасность — МИБ» за счет всестороннего продвижения и популяризации на переговорных и дискуссионных площадках наработок ГПЭ ООН и одноименных Резолюций Генеральной Ассамблеи ООН, принимаемых ежегодно с 1998 г., а с 2005 г. — с учетом наработок ГПЭ.

В частности, речь идет о терминологии «обеспечение безопасности при/в сфере использовании (-я) информационных и коммуникационных технологий (ИКТ)» (английский вариант — *security of and in the use of information and communication technologies (ICTs)*) как нейтральном и неполитизированном консенсусном термине с широким объемом.

4. Поддержка и реализация мер в части консенсусной терминологии, включенных в Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования ИКТ, который был согласован и принят 3 декабря 2013 г. при активном участии России.

Конкретно речь идет о статье 9 упомянутого перечня, в которой предлагается:

- каждому государству представить на добровольной основе перечень используемых ими терминов, касающихся безопасности ИКТ и их использования, сопровождаемый пояснением или определением по каждому термину;
- государствам-участникам — в среднесрочной перспективе составить общий согласованный глоссарий критических терминов ИКТ в сфере международной безопасности.

Целесообразной также видится организация аналогичной работы в части терминологии в рамках некоторых других форматов, в частности Регионального форума АСЕАН (АРФ) и упомянутой ГПЭ ООН.

Возможная цель к 2017 г.

Разработка и принятие в формате рекомендательного документа ООН единообразного перечня критической терминологии по вопросам ИКТ и их использования в области международной безопасности с учетом наработок ОБСЕ, АСЕАН, ГПЭ ООН и других международных форматов.

5. В тех случаях, когда консенсусные терминологические наработки не работают либо отсутствуют в дипломатической практике, целесообразно опираться на наработки и технологически ориентированные определения международных организаций прежде всего в рамках структуры ООН.

Полезен может быть опыт Международной организации по стандартизации (ИСО), которая, несмотря на статус НПО, ведет деятельность в 164 странах мира и играет важную роль в разработке и распространении стандартов; в числе ее наработок — стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности», принятый в 2012 г.

6. Наконец, преодоление терминологических конфликтов по вопросам ИКТ и их использования невозможно без обмена мнениями между представителями экспертных сообществ различных стран и регионов. В дополнение к работе правительственных экспертов в рамках ГПЭ ООН необходимо также усиление *трека 1,5* и *трека 2* в части работы над критической терминологией ИКТ.

Успешный проект такого рода был осуществлен в 2011 г. Институтом «Запад–Восток» и Институтом проблем информационной безопасности МГУ им. М.В. Ломоносова. По итогам общения группы российских и американских экспертов был издан двуязычный перечень 20 критических терминов в сфере кибербезопасности с расшифровкой. Представляется возможным возобновить подобный формат и усилить его за счет вовлечения широкого круга как правительственных, так и неправительственных экспертов из России, США и других стран. ПИР-Центр будет готов подключиться в такой работе в ближайшее время.

7. Несмотря на противоречие концепции Стратегии кибербезопасности России действующим доктринальным документам и нормативным актам, в экспертном сообществе сохраняется запрос на тот угол зрения на проблемы безопасности в сфере использования ИКТ, который отражен в ней. Востребованы серьезное обновление и доработка этого документа при участии всех профильных ведомств. К этой работе могли бы подключиться Совет по кибербезопасности при Военно-промышленной комиссии и межведомственная рабочая группа по информационной защите, о создании которых в марте 2015 г. отдал поручение заместитель председателя правительства России Дмитрий Рогозин.

Возможным направлением действий в этой связи могло бы стать формирование новой рабочей группы, включающей представителей государственных органов (СБ РФ, МИД РФ, ФСБ РФ, Министерства обороны РФ, МВД РФ, Министерства связи и массовых коммуникаций РФ и проч.), а также представителей частного сектора, академического и технического сообщества. Задача этой группы может включать проработку вариантов гармонизации терминологии концепции Стратегии кибербезопасности РФ с российским национальным законодательством и доктринальными документами.

Дополнительная информация

1. Якушев М. Интернет-2012 и международная политика // Индекс безопасности. 2013. № 1 (104). С. 29–42.
2. Материалы круглого стола ПИР-Центра «Международная информационная безопасность и глобальное управление Интернетом: взгляд российских и международных экспертов на встрече в Женеве» // Индекс безопасности. 2013. № 1 (104). С. 185–206.
3. Двусторонний проект Россия–США по кибербезопасности. Основы критически важной терминологии / Под ред. К.Ф. Раушера, В. Ященко. Институт проблем информационной безопасности МГУ им. М.В. Ломоносова, 2011. URL: http://iisi.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%20RUS.pdf (дата обращения: 01.03.2016).

Документы

1. Решение Организации по безопасности и сотрудничеству в Европе (Постоянный совет) от 03.12.2013 № 1106 «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий». URL: http://www.osce.org/ru/pc/109648?download=true (дата обращения: 01.03.2016).
2. Тунисская программа для информационного общества. Всемирная встреча на высшем уровне по вопросам информационного общества. Женева, 2003 г. — Тунис, 2005 г. Организация Объединенных Наций. URL: http://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения: 01.03.2016).
3. X.1205 (04/2008) «Обзор кибербезопасности». Серия X: Сети передачи данных, взаимосвязь открытых систем и безопасность. Международный союз электросвязи. Апрель 2004 г. URL: http://www.itu.int/rec/T-REC-X.1205-200804-I (дата обращения: 01.03.2016).
4. ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности». Всемирная организация по стандартизации. 16.07.2012. URL: http://www.iso.org/iso/ru/catalogue_detail?csnumber=44375 (дата обращения: 01.03.2016).

5. Конвенция об обеспечении международной информационной безопасности (концепция). Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 01.03.2016).
6. Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. NATO Cooperative Cyber Defense Centre of Excellence. URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf (дата обращения: 01.03.2016).
7. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/114.html (дата обращения: 01.03.2016).
8. Концепция стратегии кибербезопасности Российской Федерации (проект). Официальный сайт Совета Федерации Федерального Собрания Российской Федерации, 10.01.2014. URL: http://council.gov.ru/press-center/discussions/38324/ (дата обращения: 01.03.2016).

Раздел III

В современных военных конфликтах растет значение информационных технологий. Так называемые информационные атаки уже применяются для решения задач военно-политического характера. Причем, по оценкам специалистов, их так называемая поражающая сила может быть выше даже, чем от обычных видов оружия. Нужно быть готовыми эффективно парировать угрозы в информационном пространстве, повысить уровень защиты соответствующей инфраструктуры, прежде всего информационных систем стратегических и критически важных объектов.

Выступление Президента России Владимира Путина
на заседании Совета Безопасности РФ
5 июля 2013 г.

Обеспечение безопасности объектов критической информационной инфраструктуры: основные угрозы и стратегии реагирования

Вне зависимости от мотивов неправомерных действий в сфере использования ИКТ, в отдельную категорию по своим характеристикам выдвигаются угрозы определенному классу объектов — объектам критической инфраструктуры (КИ), в том числе объектам критической информационной инфраструктуры (КИИ).

Понятия, классификация и регулирование критической информационной инфраструктуры

Первая проблема, которая имеет не только научно-теоретическое, но и сугубо практическое значение — отсутствие единообразных определений как на международном уровне, так и в регуляторных нормах и практиках значительного количества государств.

Критически важный объект — объект, нарушение или прекращение функционирования которого может привести к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения.

Критическая информационная инфраструктура Российской Федерации — совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также информационных систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка.

Проект Федерального закона
«О безопасности критической информационной
инфраструктуры Российской Федерации»
(подготовлен ФСБ РФ, текст по состоянию
на 8 августа 2013 г.)

Российская Федерация по состоянию на начало 2015 г. является одним из государств, в которых регуляторный подход к вопросам обеспечения безопасности объектов КИИ развивается, однако пока не является завершенным и в достаточной мере систематизированным. Несмотря на активное развитие нормативной базы, до сих пор законодательно не закреплен единый подход к понятию «критически важного объекта (КВО)». Кроме того, даже внутри отрасли информационной безопасности существуют различные толкования КВО на уровне документов ключевых ведомств, вовлеченных в нормотворческий и регуляторный процесс в этой сфере (Совета Безопасности РФ, ФСБ РФ, ФСТЭК РФ). Выработка общегосударственного, интегрированного и систематизированного подхода как к определениям и классификации критически важных объектов России, так и государственной политике по защите в том числе от ИКТ-угроз, должна стать четким приоритетом уже на ближайшую перспективу.

Понятие «критически важные объекты» было определено еще в Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов, утвержденной распоряжением Правительства России от 27.08.2005 № 1314-р, как «объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени». По мере развития регуляторных подходов, выработки новых ведомственных документов и законопроектов терминология в сфере защиты КВО также уточняется и развивается, но это определение закрепилось и находит отражение в более поздних нормативных актах.

Важным шагом на пути выработки согласованного подхода стала подготовка ФСБ РФ в 2013 г. проекта федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». Законопроект предлагает само понятие критической информационной инфраструктуры (КИИ) России, а также закрепляет базовые критерии ее классификации. Предлагается классификация объектов КИИ по трем уровням опасности

от высокого до низкого, а также семь критериев ее категорирования с точки зрения ее «отраслевой» значимости (экономической, экологической, социальной, для обороноспособности и для национальной безопасности России, для реализации управленческих функций и в части предоставления значительного объема информационных услуг). При этом, исходя из возможности принятия законопроекта в течение 2015 г., сами показатели критериев должны быть определены не ранее конца 2015 г. — начала 2016 г. Что особенно важно, законопроект предлагает системное видение межведомственного взаимодействия в сфере обеспечения безопасности и защиты КИИ РФ.

Излагаемые в проекте закона нормы в целом отвечают подходам, которые сформулированы в одном из наиболее проработанных международных документов по тематике защиты КИИ — Рекомендациях по защите критических информационных инфраструктур от 2008 г., выпущенных Организацией экономического сотрудничества и развития (OECD Recommendations on the Protection of Critical Information Infrastructures (2008)). При этом в российском законопроекте практически не затронута тематика международного взаимодействия по вопросам защиты КИИ, которое предусмотрено в рекомендациях ОЭСР в качестве одного из основных направлений деятельности.

Также в законопроекте не приводится полная классификация КИИ РФ, как и КВО РФ. Вопрос классификации важен как для решения внутригосударственных задач в этой сфере, так и для международного взаимодействия и сотрудничества. Отсутствие единой официально утвержденной классификации КВО и КИИ РФ осложняет межведомственное взаимодействие, служит дополнительным стимулом для конкуренции различных ведомств и регуляторов за полномочия в этой сфере, а также дезориентирует операторов самих КВО и объектов КИИ и диктует необходимость двойной и тройной отчетности об инцидентах и мерах по защите своих объектов перед различными регуляторами. Как один из примеров видения классификации КВО РФ приведем подход МЧС РФ. Нормативные акты министерства предусматривают идентификацию критической инфраструктуры по семи *видам угроз*, двум *классам угроз* и 50 *типам объектов* (зарубежным секторам приблизительно соответствует деление по семи видам угроз).

Помимо разницы во взглядах на приоритет международного сотрудничества, в повестке дня обеспечения ИБ КВО вновь проявляют себя нерешенные вопросы терминологии и классификации. Сопоставление терминологии документов Австралии, Германии, Канады, Великобритании, Нидерландов, России, США, Японии и других государств показывает существенные расхождения в логике определения таких объектов. Разные государства также выделяют различные классы/секторы КИИ (либо не выделяют таковую из общего перечня критической инфраструктуры вообще).

В США выделяются 16 секторов критической инфраструктуры; в Канаде, ЕС, Швейцарии и Японии — по 10 секторов. В большинстве случаев классификации объектов критической инфраструктуры в различных странах отличаются друг от друга, несмотря на то что значительная часть объектов (АЭС и объекты ЯТЦ, дамбы и ключевые объекты гидроэнергетики, крупнейшие телекоммуникационные инфраструктуры, правительственные информационные системы и ряд других) попадают практически во все классификации.

Однако особенностью российского подхода является то, что, в отличие от других государств, в которых объекты критической инфраструктуры, как правило, заранее распределены по отраслям, в России действует система признаков классификации объектов, относящихся к критическим. Точный перечень таких признаков не содержится в открытых источниках, однако сам принцип системы состоит именно в применении к объекту инфраструктуры системы критериев, а не отнесения его к списку КИ исключительно на основании той отрасли или сектора, к которому объект принадлежит.

В международной практике к категориям КИИ, встречающимся в классификациях абсолютного большинства государств, как правило, относятся:

- объекты атомной отрасли;
- энергосети, энергогенерирующие и энергораспределительные мощности;
- транспортные системы: авиация, железные дороги, автомобильные дороги и т. д.;
- объекты производства и хранения сельхозпродукции, а также продовольственного обеспечения;

- объекты государственного управления и правительственных коммуникаций;
- объекты ТЭК, в том числе нефтегазового комплекса;
- основные телекоммуникационные системы, сети, программно-аппаратное обеспечение и системы связи;
- объекты ОПК (в России — химически опасные объекты);
- финансово-кредитный сектор;
- водообеспечение и водоснабжение;
- здравоохранение.

Приведенный перечень, с одной стороны, показывает, что некоторые категории объектов причисляются к КИ почти во всех национальных законодательствах. С другой стороны, даже в этом случае неминуемы различия в трактовках, определениях и детализации категорий. Во многих государствах выделяются категории объектов КИ, часть из которых могут вообще не встречаться у их партнеров, и наоборот.

В то же время на международном уровне до сих пор практически нет механизмов, которые бы обеспечивали эффективное взаимодействие в сфере обеспечения безопасности КИИ. В частности, никаких специальных мер обеспечения безопасности КИИ среди прочих объектов не предусматривают ни Будапештская конвенция, ни межправительственное соглашение ШОС. Эпизоды кибершпионажа и атаки с использованием вредоносного ПО против объектов КИ периодически попадают в проработку национальными CERT и их ассоциациями, альянсом ИМПАКТ–МСЭ, иными структурами частного сектора и частно-государственного партнерства.

В рамках различных форматов за последнее десятилетие сформировалось и действует значительное число проектов, обеспечивающих взаимодействие в сфере безопасности КИИ на технологическом уровне. Такие проекты и форматы включают в себя оценку угроз, разработку и продвижение технических рекомендаций по защите объектов и прочие меры. Технические аспекты обеспечения безопасности КИИ оказались включены в деятельность Международной электротехнической комиссии (IEC), Европейского агентства сетей и информационной безопасности (ENISA), Организации экономического сотрудничества и развития (OECD) и проч.

Однако практически ни один из упомянутых форматов на сегодняшний день не обеспечивает полномасштабного международного сотрудничества, которое включало бы в себя диалог по политико-правовым аспектам обеспечения безопасности КИИ — как в контексте обмена национальным опытом, так и на уровне выработки широких международных договоренностей.

Одним из немногих исключений можно назвать Международное агентство по атомной энергии (МАГАТЭ), которое в рамках своих компетенций ведет работу по укреплению кибербезопасности объектов мирной атомной отрасли. Агентство издает технические руководства по обеспечению компьютерной безопасности на ядерных установках (серия NSS 17), а также развивает отдельные рекомендации в этой части в документах по физической ядерной безопасности (INFCIRC/225/Revision 5). При Департаменте МАГАТЭ по физической ядерной безопасности действует Программа компьютерной и информационной безопасности, в рамках которой разрабатываются технические рекомендации, публикуются документы, проводятся консультативные встречи, региональные тренинговые курсы. Среди типов угроз КИИ атомной отрасли, которые рассматриваются в рамках программы, важное место занимают целенаправленные компьютерные атаки.

Также одной из площадок, работающих над изучением международного опыта и подготовкой исследований лучших практик обеспечения безопасности КИИ, остается ОЭСР. Организацией в 2007–2008 гг. издана серия отчетов и иных документов, обобщающих анализ политик семи государств, имеющих развитые подходы к вопросам защиты КИИ. Среди ключевых выводов документов ОЭСР: необходимость развития научных и образовательных политик в части защиты КВО от ИКТ-угроз; наращивания международного взаимодействия между CERTs/CSIRTs, а также обмена информацией об угрозах и лучших практиках и развития государственно-частного партнерства. Наработки и выводы ОЭСР видится целесообразным учесть России (с учетом подготовки к присоединению к Организации) в рамках развития собственного подхода к защите КИИ.

Среди региональных форматов активной проработкой проблем обеспечения безопасности КИИ выделяются ОБСЕ, АСЕАН/АРФ, а также АТЭС. В 2013 г. ОБСЕ подготовила «Руководство по передовой практике защиты важнейших объектов неядерной энер-

гетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства». Документ содержит перечень рекомендаций по развитию международного сотрудничества в рамках указанной проблематики.

Среди государств к числу лидеров в регулировании вопросов безопасности КИИ следует отнести США, Великобританию, Германию, Австралию и Японию. В Соединенных Штатах одним из ключевых национальных регуляторов по вопросам КИИ сегодня выступает Национальный институт стандартов и технологий (NIST). Институт со временем вобрал передовые наработки Министерства энергетики США и некоммерческой организации, разработавшей большое количество стандартов в области электротехники, — Североамериканской корпорации по надежности электроэнергетики (NERC).

В феврале 2014 г. NIST издал основополагающий Рамочный документ по укреплению кибербезопасности критической инфраструктуры (Версия 1.0). Цель такого документа была сформулирована годом ранее, в приказе президента США Барака Обамы № 13636 «Укрепление кибербезопасности КИ», она включает в себя создание системы стандартов, руководств и практик для содействия структурам частного и государственного сектора в управлении рисками в сфере ИКТ. Документ NIST является одним из актов в сфере обеспечения безопасности КИИ, который позиционируется в качестве модели международного сотрудничества и предлагается к использованию зарубежными организациями. Предполагается, что документ может способствовать «выработке общего языка международного сотрудничества в обеспечении безопасности КИИ». Еще один документ NIST, который детально рассматривает вопросы безопасности КИИ, — Руководство по защите АСУ ТП NIST SP800-82, изданное в 2011 г. Обширная и глубокая проработка NIST вопросов ИКТ-безопасности объектов КВО делает актуальной задачей учет опыта ведомства США при выработке международных практик и документов по вопросам безопасности КИИ.

В рамках практических, прикладных форматов международного взаимодействия растет роль киберучений, специализированных на критической инфраструктуре.

Крупнейшие общеевропейские киберучения под названием *Cyber Europe* с 2010 г. каждые два года проводит Европейское агентство

сетевой и информационной безопасности (ENISA). Очередные, третьи, учения ENISA начались 29 апреля 2014 г. с участием 29 команд стран — членов ЕС и более 400 специалистов; главной задачей учений было выявление слабых мест и возможностей для укрепления КИИ ЕС в рамках технической, оперативно-тактической и стратегической фаз. Отражение угроз КИИ, исходящих от компьютерных атак и использования ИКТ в неправомерных целях, также является одной из основных целей учений НАТО Cyber Coalition, которые в 2013 г. вовлекли более 300 специалистов из 30 стран, включая четырех партнеров, не являющихся членами НАТО. В рамках учений угрозы КИИ и противодействие им напрямую увязывается с вопросами кибероборонны.

Другим редким примером механизма по развитию норм и подходов к обеспечению безопасности КИИ является проект Модельного закона о КВО информационно-коммуникационной инфраструктуры, разработанный в рамках СНГ в 2013 г. Из числа механизмов, выработанных в рамках СНГ, стоит упомянуть и «Рекомендации по совершенствованию и гармонизации национального законодательства государств — участников СНГ в сфере обеспечения информационной безопасности», утвержденные постановлением МПА СНГ от 23.11.2012 № 38-20. Вместе с тем, предоставляя странам СНГ рекомендации и общие ориентиры для развития регулирования на национальном уровне, такие документы не формируют напрямую регуляторные механизмы и сами по себе не ведут к появлению новых инструментов международного взаимодействия и сотрудничества по вопросам КИИ. Следует также отметить, что роль СНГ как площадки интеграции и выработки общих политик в последние годы снижается как за счет внутрирегиональных кризисов и конфликтов («Пятидневная война» в 2008 г., вооруженный конфликт на Востоке Украины 2014–2015 гг.), так и в силу роста интереса правительств к альтернативным трекам региональной интеграции (Евразийский Союз).

Некоторые другие региональные форматы в последние годы также начали активно обсуждать перспективы совместного противодействия угрозам информационной безопасности критических инфраструктур и возможностей выработать некие коллективные механизмы в этой сфере.

Преимущественное отсутствие нормативных механизмов международного взаимодействия и обмена информацией об ИКТ-атаках

на объекты КИИ объясняется несколькими причинами. Возможно, ключевая из них — новизна самой проблематики, причем не только в международной повестке дня, но и на внутригосударственном уровне регулирования. Вопросы, связанные с проработкой проблем ИБ КВО и ИБ АСУ ТП, в том числе в части изоляции таких объектов от Интернета и их защиты от компьютерных атак извне, даже в экономически передовых и развитых странах выдвинулись на передний план для индустрии и регуляторов лишь в течение последнего десятилетия. Устойчивой предпосылкой для активного развития международного сотрудничества зачастую выступает завершенное, четкое видение проблемы и стратегий ее решения на уровне отдельных участников диалога, что в случае с обеспечением безопасности КИИ верно далеко не для всех государств.

Безусловно, в последние годы ситуация меняется очень быстро, но к такому темпу изменений готовы не все и не во всех странах. Как Россия, так и ее зарубежные партнеры все острее сталкиваются с дефицитом интеллектуальных ресурсов, готовых специалистов по ИБ АСУ ТП, а также с частичным регуляторным вакуумом, который проявляется в нехватке существующих стандартов, технических рекомендаций и нормативов в этой области. Как итог, международное сотрудничество в этой области пока не в полной мере обеспечено ресурсами и подкреплено осознанными стратегиями своих участников, чтобы активно и продуктивно развиваться.

Вторая причина связана с особым режимом безопасности объектов КИИ. Соображения национальной безопасности и режимы ограничения доступа к информации об объектах КИИ действуют практически во всех странах. Вследствие этого международное сотрудничество в полноценном понимании этого термина требует качественно иного уровня доверия между его сторонами и потому в обозримой перспективе сильно ограничено по своему потенциалу. Речь может идти о формировании на международном уровне общего понимания ИКТ-угроз КИИ и организации доступа к лучшим мировым практикам и внешним ресурсам для противодействия им. Контуры и задачи участников такого взаимодействия должны отражать актуальную картину угроз в этой сфере.

Наконец, обострение отношений России с рядом стран Запада, а также приостановка ряда механизмов обмена информацией

и сотрудничества в сфере безопасности, включая вопросы ИКТ, едва ли будет способствовать конструктивной выработке механизмов международного взаимодействия в области безопасности КИИ.

Позитивной возможностью даже в отсутствие условий для выработки норм, укрепляющих международное сотрудничество, видится развитие взаимодействия и обмена информацией между Центрами реагирования на компьютерные инциденты (CERT/CSIRT). В России существует уже несколько таких центров — как государственных (RU-CERT, GOV-CERT), так и частных. Одним из примеров частных центров реагирования на компьютерные инциденты является GIB-CERT, созданный компанией Group-IB и до последнего времени остававшийся единственным российским CERT, обеспечивающим круглосуточное и полнофункциональное взаимодействие по реагированию на киберинциденты как российских, так и международных клиентов. В 2015 г. GIB-CERT оказался единственным российским Центром реагирования на киберинциденты, который получил аккредитацию как член FIRST — крупнейшего международного сообщества центров реагирования на инциденты кибербезопасности. Кроме того, GIB-CERT является участником альянса ИМПАКТ-МСЭ, а также аккредитованным членом сообщества Trusted Introducer, объединяющего европейские центры реагирования на киберинциденты. Глубокая интеграция в структуры международного взаимодействия и обмена данными по киберинцидентам, в том числе и в отношении КВО и объектов КИИ, существенно расширяет возможности GIB-CERT. Кроме того, пример центра GIB подчеркивает огромную роль частного сектора в защите объектов КИИ и реализации государственной политики в этой сфере. Даже при том, что Россия далека от США по показателю доли частного сектора среди владельцев и операторов объектов КВО (в США — более 80%), компетенции бизнеса, частного сектора незаменимы и необходимы для построения эффективного механизма защиты критической инфраструктуры от ИКТ-угроз.

Также стоит отметить, что в последнее время в России наметилась еще одна тенденция, уже получившая глубокое развитие в США, ряде стран Европы и Юго-Восточной Азии: создание специализированных «отраслевых» центров реагирования на киберинциденты. Такие структуры уже есть не только в США, где существуют собственные центры реагирования на компьютерные

инциденты крупных банков (например, CIRT Bank of America) и специализированные отраслевые структуры (Financial Services Information Sharing and Analysis Center, FS-ISAC), но и во многих других странах. Лишь в списке участников FIRST (международный Форум команд обеспечения безопасности и реагирования на киберинциденты), к примеру, присутствуют CIRT 17 банков, в том числе Canadian Imperial Bank of Commerce, Commerzbank (ФРГ), Европейского Центрального банка, First National Bank (ЮАР), Deutsche Bank, Handelsbanken (Швеция), Национального банка Австралии.

Естественно, специализированный подход важен прежде всего в контексте защиты КИИ, поскольку позволяет регуляторам, государственным и частным структурам сфокусировать свои усилия на предотвращении и реагировании на компьютерные инциденты в том или ином конкретном секторе критической инфраструктуры. С 1 июля 2015 г. при Центральном Банке РФ начал работу Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FINCERT). Одна из главных задач Центра состоит в накоплении информации об инцидентах в банковском секторе и потенциальных угрозах и ее распространении среди организаций российского банковского сектора. Ключевые объекты финансовой и банковской инфраструктуры в большинстве стран мира, безусловно, относятся к числу КВО, и угрозы кибербезопасности в этой нише носят постоянный и системный характер. Важно, чтобы методика работы и круг задач FINCERT по мере развития и накопления его компетенций включали в себя приоритет международного взаимодействия с другими центрами, занимающимися реагированием и предупреждением инцидентов в финансово-кредитном секторе. Теоретически мало что мешает организовать схему обмена данными об инцидентах и даже аномалиях трафика в банковских сетях в международном масштабе — технические вопросы сводятся к стандартизации формата и выбору каналов обмена данными (например, таких как используемый FS-ISAC Traffic Light Protocol (TLP)).

Наконец, запуск FINCERT представляет собой позитивный пример, запрос на воспроизведение которого может быть и в других секторах и отраслях национальной экономики и управления, опирающихся на КВО и объекты КИИ: транспортно-логистическом секторе, авиаперевозках, электроэнергетике, медицине и проч.

Информационные угрозы объектам КИИ: основные тенденции развития

В целом перечень угроз промышленным системам управления, в том числе АСУ ТП объектов КИ, раскрывается в разработанном Организацией по безопасности и сотрудничеству в Европе Руководстве по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства.

Согласно этому руководству основными угрозами системам контроля технологических процессов (ICS) на объектах критической инфраструктуры вследствие преднамеренных неправомерных действий являются:

- Несанкционированное использование точек доступа дистанционного технического обслуживания (специальные внешние входы в сеть ICS, которые могут быть недостаточно защищены).
- Сетевые атаки через корпоративную сеть.
- Атаки на стандартные компоненты, используемые в сети системами контроля технологических процессов (ICS) (в частности, могут эксплуатироваться уязвимости системного программного обеспечения, сервер приложений или баз данных).
- (D)DoS-атаки (возможны при наличии подключения ICS к Интернету).
- Саботаж со стороны внутренних и внешних нарушителей (в данном случае речь не идет о саботаже средствами специального ПО).
- Запуск вредоносного ПО через съемные носители и внешние устройства (Stuxnet).
- Чтение и запись записей в сети промышленных систем контроля (АСУ ТП).
- Несанкционированный доступ к ресурсам.
- Атаки на компоненты сети (атака типа «незаконный посредник» (MITM), упрощение анализа трафика и проч.).

В основных параметрах динамика ИКТ-угроз объектам КИИ сегодня может быть описана в рамках нескольких тенденций:

- Рост числа и масштабов инцидентов, связанных с ИКТ-угрозами АСУ ТП КВО.

- Внедрение интеллектуальных систем энергоснабжения (программа Smart Grid) и неуклонное повышение зависимости функционирования КВО от АСУ ТП в целом информационных систем, в том числе подключенных к различным сетям, в том числе и Интернету.
- Тенденция к увеличению числа инцидентов, предположительно отражающих стратегические мотивы нарушителей, в том числе и в пользу отдельных государств.
- Стратегия сочетания инструментов кибершпионажа и агрессии при осуществлении недружественного воздействия на АСУ ТП КВО.

Отдельного внимания заслуживает резкий рост количества и размаха кампаний кибершпионажа и целевых атак в отношении объектов КИИ (см. рис. 5).

На рисунке 5 приведены далеко не все примеры кампаний кибершпионажа и организации атак с использованием ИКТ на объекты КИИ.

Тем не менее, несмотря на глобальный масштаб кибершпионажа в отношении объектов КИИ, еще бóльшую и прямую угрозу может представлять использование различных вредоносных программ для вмешательства в работу информационных систем объектов КИ, в том числе саботажа функционирования таких объектов.

На сегодняшний день наиболее известным и серьезным по своим последствиям инцидентом, связанным с умышленными атаками на объекты КИИ с использованием специально разработанного программного обеспечения, остается использование червя Stuxnet для саботажа работ по обогащению урана на комбинате в иранском г. Натанз в 2009–2010 гг.

Помимо беспрецедентной сложности и успешного саботажа объектов в Натанзе, дополнительную опасность Stuxnet придало быстрое распространение по всему миру после попадания червя в Глобальную сеть в 2010 г. Несмотря на то что заражение десятков тысяч устройств не повлекло серьезных последствий в силу того, что вирус был нацелен на ПЛК одной конкретной модели, «утечка» червя в Глобальную сеть показала, что даже самые точные и сложные инструменты операций с использованием ИКТ могут выходить из-под контроля и угрожать неограниченно широкому кругу объектов.

1999–2000 гг.
Moonlight Maze

Целевая хакерская атака.
Целями стали объекты на территории США, прежде всего сети Пентагона, NASA, Министерства энергетики, а также частных лабораторий и исследовательских университетов. Началась в 1998 г., продолжалась до конца 2000 г. Результат: похищены десятки тысяч файлов, включая военные карты Пентагона и схемы военной и специальной техники. США отследили источник до серверов в РФ, однако доказательств прямого российского участия нет. Пресса США впервые назвала ситуацию «кибервойной».

2003–2005 гг.
Titan Rain

Серия атак на сети ключевых структур оборонного сектора США. До операции «Олимпийские игры» считалась одной из наиболее масштабных кибератак в истории. Началась в 2003 г., продолжалась не менее трех лет. Уровень подготовки и исполнения

2006–2010 гг.
Stuxnet

Средство стратегического саботажа иранской ядерной программы, первое в истории оружие на основе ИКТ. Часть «Олимпийских игр» (подробнее см. ниже).

2006–2012 гг.
Flame

Вредоносное ПО, средство кибершпионажа. Считается частью «Олимпийских игр». Более 20 модулей, общий объем до 20 МБ. Могло разрабатываться и применяться с 2006 г. Выявлено «Лабораторией Касперского» в июне 2012 г. Заразило более 1000 устройств, более 65% на Ближнем Востоке, большинство в Иране. Цель: данные, связанные со стратегическими отраслями, в том числе атомной.

2007–2012 гг.
Red October (Красный октябрь)

Глобальная кампания кибершпионажа (серия целевых атак). Выявлена «Лабораторией Касперского» в январе 2013 г., могла вестись с 2007 г. Цель: дипломатически и политически значимые сведения. За пять лет жертвы: правительственные и дипломатические ведомства, посольства, исследовательские институты, военная и аэрокосмическая отрасли, организации энергетического сектора (ядерные и нефтегазовые, торговые и коммерческие структуры). Более 300 случаев заражения, более 20 стран мира, на первом месте Россия.

2007–2013 гг.
Программа «Олимпийские игры»

Масштабная операция по разработке, испытанию и внедрению в целевые объекты линейки передового вредоносного ПО для сбора информации об иранской ядерной программе, а также ее саботаж и максимальное торможение. Включает такие программы, как Stuxnet, Duqu, Flame, Gauss. Активная фаза реализации: 2007–2013 гг. В подготовке и проведении программы обвиняются ЦРУ, администрация президента США и спецслужбы Израиля, обвинения в адрес США не были опровергнуты.

Рис. 5. Некоторые крупные акции кибершпионажа и похищения чувствительных данных в 1999–2014 гг.

заставил американцев подозревать участие государства, обвиняется КНР. В результате атаки похищены до 10 Тб несекретных, но чувствительных данных из внутренних сетей Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, а также NASA.

2005–2011 гг.
Ghost Net

Глобальная кампания кибершпионажа. Поражала системы на территории 103 государств. Наибольшее количество атак пришлось на Тайвань, Вьетнам и США. Обнаружена и описана в марте 2009 г., могла применяться с 2005–2006 гг. В 2011 г. все еще была активна и поражала системы. Цели: системы государственных учреждений: посольств, МИД, финансовых структур в правительствах различных стран, правительство Тибета в изгнании. В кампании обвинялись власти КНР, однако бездоказательно.

2008–2011 гг.
DuQu

Узконаправленная операция кибершпионажа и одноименное вредоносное ПО. Считается частью «Олимпийских игр». Создано к 2008 г. с использованием исходного кода Stuxnet. Выявлено в сентябре 2011 г. Поражало персональные устройства и корпоративные сети в основном в странах Ближнего Востока, включая Иран. Вероятная цель: сбор информации о ядерной программе Ирана для ее последующего саботажа при помощи Stuxnet.

2009–2010 гг.
Operation Aurora

Кампания целевых атак на инфраструктуру ведущих компаний ВПК и интернет-сектора США. Осуществлялась с июня 2009 г. по февраль 2010 г. Использовались реинжинируемые наборы эксплоитов и уязвимости нулевого дня. В числе пострадавших были Adobe Systems, Juniper Networks, Rackspace, Yahoo, Symantec, Juniper Networks, Adobe, Northrop Grumman и Dow Chemical. США обвинили хакеров из Подразделения НОАК 61398 в атаке с санкции Политбюро КПК по политическим мотивам. Одной из основных целей был Google, чья интеллектуальная собственность была похищена. После атаки Google заявил о возможном уходе с китайского рынка.

2011–2012 гг.
Gauss

Модульное вредоносное ПО, используется для кибершпионажа. Действовало с сентября 2011 г., выявлено в июне 2012 г. Могло быть разработано на основе исходного кода Stuxnet и Flame в рамках операции «Олимпийские игры». В географии заражений преобладает Ближний Восток. Цель: похищение данных о стратегических отраслях промышленности.

Stuxnet — первый прецедент применения вредоносного ПО в целях саботажа стратегических объектов

Описание. Компьютерный червь, первое в истории орудие стратегического саботажа средствами ИКТ. Многими российскими и зарубежными экспертами признан первым случаем использования компьютерного кода в качестве оружия, обсуждалась теоретическая возможность квалификации его использования в качестве акта агрессии в рамках Статьи 52 Устава ООН.

Создание и применение. Разрабатывался с 2005–2007 г. в рамках программы *Олимпийские игры* как средство замедления иранской атомной программы тайными невоенными средствами. В 2008–2010 гг. поразил АСУ ТП на комбинате по обогащению урана в иранском городе Натанз. Первая версия червя могла поразить иранские объекты в 2007 г.; обновленные версии появлялись в июне 2009 г., а также весной 2010 г., также попав в сети объекта в Натанзе. Выявлен лишь 17 июня 2010 г. после многих месяцев скрытой деятельности. Активность червя привела к физическому износу и выведению из строя более 1000 центрифуг и торможению ядерной программы Ирана на срок от шести месяцев до двух лет. Эти события спровоцировали широкую дискуссию о потенциале использования кибероружия и необходимости его ограничения.

Функционал. Крайне передовая и сложная вредоносная программа объемом более 500 Кб, 15 000 строк кода. Осуществлял перехват и модификацию информационного потока между программируемыми логическими контроллерами (ПЛК) Siemens марки Simatic S7 и рабочими станциями системы Simatic WinCC. Использовал четыре уязвимости нулевого дня ОС Microsoft Windows и два действительных цифровых сертификата. Возможно, распространялся через USB-накопители, после попадания во внутреннюю сеть скрытно распространялся, находил нужные ПЛК, перехватывал контроль над ними и (в случае с Натанзом) изменял скорость вращения роторов центрифуг, вызывая их ускоренный физический износ. В то же время на рабочие станции АСУ ТП отсылалась заранее сохраненная червем информация о штатной работе всех центрифуг, что позволяло Stuxnet в течение долгого времени действовать скрытно.

Учитывая опыт Stuxnet, необходимо понимать, что инцидент в Натанзе не стал единичным примером использования ИКТ для нарушения работы объектов КИИ, а спектр ИКТ-угроз таким объектам не исчерпывается операциями государственных игроков с мотивами стратегического саботажа. За последние годы в открытом доступе неоднократно появлялись сообщения об инцидентах, связанных с вмешательством в работу объектов КИИ в различных секторах национального хозяйства, включая атомную отрасль:

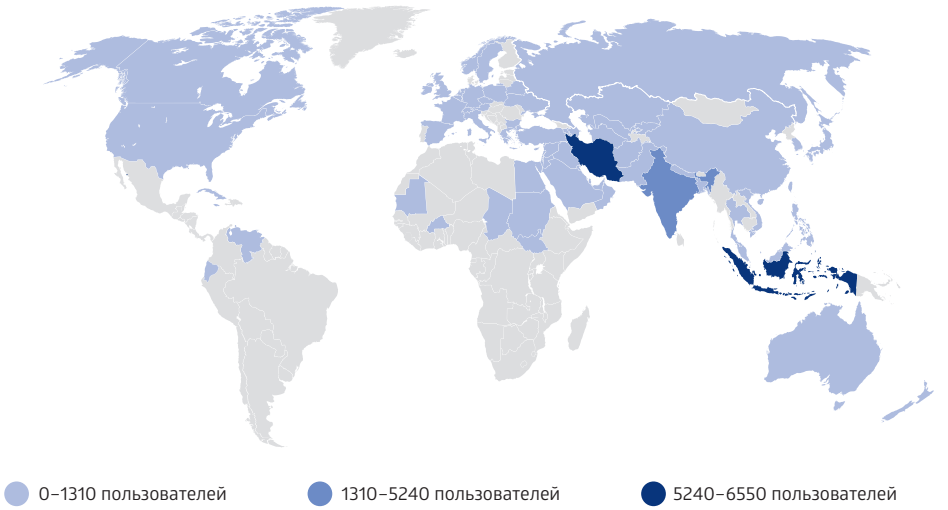


Рис. 6. География заражений Stuxnet пользовательских устройств и сетей после попадания в Интернет в 2010 г.

Источник: UMBC Embuquity

- В США в 2003 г. червь Slammer проник на АЭС Дэвис Бесс (Davis-Besse) и вызвал сбой в цифровой системе мониторинга параметров безопасности, проникнув из внешней сети на АСУ ТП станции. Дублирование функций мониторинга аналоговой системой позволило персоналу объекта получать необходимые данные о состоянии на протяжении почти пяти часов сбоя и избежать серьезных последствий.
- К кампаниям и образцам ПО на рисунке 5 достаточно близок *троян*, известный как Shamoon и использовавшийся для атак на инфраструктуру нефтяных компаний Саудовской Аравии и, предположительно, Катара. В августе 2012 г. червь мог заразить до 30 000 рабочих устройств арабской нефтяной компании Saudi Aramco; в сентябре 2012 г. похожая атака имела место в отношении катарской компании по производству СНГ RasGas. Несмотря на «родство» с Flame и похожего модульного дизайна, Shamoon, согласно отчету «Лаборатории Касперского», предназначен не для сбора информации, а для уничтожения файлов на зараженных системах. Для ликвидации последствий заражения червем предприятие Saudi Aramci было вынуждено

приостановить работу внутренней корпоративной сети на десять дней и понесло определенные убытки. Хотя Shamoon не может быть назван инструментом саботажа КИИ (червь не проник в АСУ ТП), такой инцидент все же затрагивает работу критических объектов.

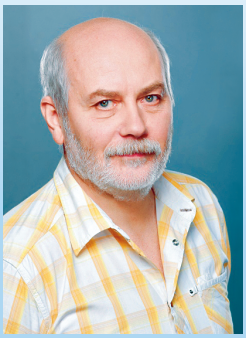
Ключевые выводы, которые позволяет сделать сегодняшняя картина инцидентов безопасности КИИ в части ИКТ-угроз, неутешительны:

- Нарушение работы стратегических объектов, включая техногенноопасные объекты, средствами ИКТ технически реально и в определенных обстоятельствах политически приемлемо для ряда ключевых игроков, включая государства.
- Даже при наличии большого количества косвенных технических данных, указывающих на заказчика кибератаки на критический объект, и подтверждения такой информации независимыми источниками (Эдвард Сноуден, Дэвид Сангер) оперативное трансграничное расследование инцидента малореально, так как возможности и механизмы достоверной атрибуции атак на международном уровне крайне ограничены. Это обеспечивает безнаказанность государств и субъектов-посредников, причастных к таким атакам.
- Несмотря на соображения национальной безопасности, государствам, осуществляющим эксплуатацию техногенноопасных объектов КИ, по мере роста роли ИКТ в эксплуатации таких объектов все более остро нужен будет доступ к лучшим мировым практикам и экспертизе в сфере обеспечения безопасности КИИ. Прежде всего речь идет о развивающихся странах, активно воплощающих программы строительства техногенноопасных объектов, включая объекты атомной отрасли (Индия, Вьетнам, Иран, Турция, Бангладеш, Пакистан), либо планирующих их развитие (Алжир, Египет, Индонезия и проч.). Собственных компетенций в случае атак, аналогичных либо превосходящих по уровню сложности Stuxnet, специалистам таких стран может не хватить, как показывает иранский опыт. В ситуации, когда выработка форм конструктивного международного взаимодействия может оказаться затруднительной в нынешних условиях, более вероятными могут оказаться двусторонние или региональные форматы такого сотрудничества.

- Отсутствие реализованной угрозы Бушэрской АЭС в случае со Stuxnet не означает того, что выведение таких объектов из строя невозможно. В 1988 г. на Игналинской АЭС в Прибалтике был зафиксирован случай саботажа со стороны работника отдела АСУ, который внес изменения в работу программного комплекса, отвечающего за один из процессов на атомном реакторе. По счастливой случайности жертв удалось избежать. В этой связи необходимо не только признание, но и отражение нового вида и уровня риска в политиках и документах государств, осуществляющих эксплуатацию АЭС и других техногенноопасных объектов (иные объекты ЯТЦ, дамбы ГЭС и проч.).

Эти факторы, с учетом отсутствия у значительной части государств эффективных стратегий борьбы с изощренными ИКТ-угрозами безопасности КИИ и дефицита кадров, экспертных компетенций и иных ресурсов у многих развивающихся стран, ставят вопрос о развитии международного взаимодействия в сфере обеспечения безопасности объектов КИИ.

Актуальность обеспечения защиты АСУ ТП от информационных угроз



Андрей Духвалов, руководитель управления перспективных технологий «Лаборатории Касперского»
Работает в «Лаборатории Касперского» с 1998 г. За время работы прошел путь от инженера-программиста до главного архитектора ПО. В настоящее время возглавляет Департамент перспективных технологий. Участвовал в разработке ряда прорывных технологий и продуктов «Лаборатории Касперского». Сейчас занимается разработкой защищенной операционной системы и технологий, предназначенных для защиты АСУ ТП.

Необходимость информационной защиты автоматизированных систем управления технологическими процессами (АСУ ТП) в настоящее время уже не подвергается сомнению со стороны ведущих мировых специалистов. Тем не менее все еще достаточно широко распространено мнение, что подобные системы не нуждают-

ся в защите или изначально неплохо защищены. Кроме того, некоторые специалисты уверены, что имеющиеся сегодня средства защиты не могут быть использованы в индустриальной информационной среде.

Отчасти такие сомнения оправданны — существующие средства информационной защиты действительно необходимо применять в индустриальной среде с большой осмотрительностью, однако пренебрегать защитой ни в коем случае нельзя. Совершенно ясно, что в современных условиях информационные технологии могут быть использованы для негативного воздействия на индустриальные объекты, вплоть до нанесения значительного материального ущерба и даже до физического разрушения. Несколько таких случаев уже было зафиксировано.

Разумеется, подходы к информационной безопасности АСУ ТП существенно меняются по сравнению с «офисной» информационной средой или использованием информационных технологий в личных целях. Если для рядовых пользователей приоритетом является конфиденциальность информации, а целость и доступность данных имеют меньшую значимость, то в технологических системах управления приоритеты другие, и первостепенное значение здесь имеют как раз целостность и доступность данных, благодаря которым и обеспечивается непрерывность процесса управления.

Новая реальность

Нарушить стабильность функционирования производственной сети сегодня может не только отказ технологических узлов или ошибка оператора, но также ошибки в ПО, случайное заражение рабочих станций вредоносными программами или целенаправленные действия со стороны киберпреступников. А они в последние годы проявляют все больший интерес к инфраструктурным и промышленным объектам.

Например, с 2010 г. и по настоящее время продолжается кампания кибершпионажа, известная как Crouching Yeti или Energetic Bear. Более 2800 предприятий, значительная часть которых связана с энергетикой и машиностроением, уже пострадали от действий организаторов этой операции — предположительно похищена конфиденциальная информация, составлявшая коммерческую тайну. Большая часть предприятий-жертв находится

в США и Испании, однако в их числе есть и некоторые российские объекты.

Другой пример: 2 января 2014 г. системный администратор японской АЭС Monju обнаружил многократные удаленные подключения к одному из восьми компьютеров в центре управления реактором. Причиной этого инцидента стала установка одним из сотрудников обновления бесплатного видеоплеера GOM Media Player. В результате инцидента злоумышленниками была украдена часть информации, в том числе конфиденциальной, хотя последствия исполнения злонамеренного программного кода в центре управления реактором могли бы быть куда более опасными.

Казалось бы, в этих условиях достаточно обеспечить сетевую изоляцию АСУ ТП. Но несостоятельность этой концепции продемонстрировал печально известный инцидент с Stuxnet: компьютерный червь размером 500 Кб проник в изолированные сети через USB-накопитель и инфицированные SCADA-проекты, заразил программируемые логические контроллеры и физически вывел из строя центрифуги на ядерном объекте в Иране. Более того, потом этот червь «вырвался на свободу» и затронул ряд других критически важных объектов.

В конце 2014 г. также была зафиксирована атака на одно из металлургических предприятий в Германии. При помощи фишинга и методов социальной инженерии, в частности посредством писем, содержавших вредоносные вложения, киберпреступники проникли во внутреннюю сеть предприятия и получили доступ к системам управления производством. Инцидент привел к тому, что сталеплавильную печь невозможно было остановить в штатном режиме, что привело к значительным убыткам. Это второй случай после Stuxnet, когда проникновение вредоносного ПО в АСУ ТП закончилось для предприятия реальным материальным ущербом.

Однако АСУ ТП критически важных объектов угрожают не только целенаправленные атаки со стороны кибертеррористов. Специфика этих систем такова, что они вполне могут пострадать и от самых обычных, «офисных» вирусов. Однако в промышленных сетях обычное вредоносное ПО способно причинить несравнимо больший вред, чем при заражении офисного или домашнего компьютера — например, заблокировать выполнение критически важных приложений, что приведет к сбою в работе оборудования.

Например, червь Conficker сумел заразить производственную сеть только потому, что в ней не было своевременно установлено обновление ОС Windows.

Зловред посылал миллионы сетевых запросов, тем самым вызывая паралич производственной сети.

Даже средства автоматизированного проектирования могут использоваться для распространения вредоносного кода. Так, например, был зарегистрирован случай проникновения в производственную сеть вредоносной программы, написанной на языке AutoLisp (AutoCAD). Она внедрила вредоносный код в чертеж, открытие которого привело к массовому уничтожению данных.

Обеспечение непрерывности процесса управления АСУ ТП

Основным показателем защищенности АСУ ТП является их способность поддерживать стабильность, непрерывность и корректное функционирование технологического процесса, будь то выработка и передача электричества, очистка воды, управление производством или что-то другое, независимо от внешних воздействий. Но в реальной жизни всегда существует масса факторов, из-за которых промышленные системы могут выйти из строя, особенно если им «помогают» киберпреступники.

Наибольшему риску АСУ ТП сегодня подвергаются в первую очередь из-за устаревшего ПО, оборудования и коммуникационных протоколов, изначально не предполагавших даже самой возможности существования киберугроз. Проблема усугубляется еще и тем, что для обновления этого ПО нужно преодолеть массу административных и технологических трудностей, и не каждая компания пойдет на это.

Немало вопросов вызывает также информационное взаимодействие сети АСУ ТП с офисной сетью предприятия. Обычно АСУ ТП функционируют в изолированной сети, но нередки случаи, когда в ней создаются каналы обмена информацией с корпоративной сетью для обеспечения тех или иных производственных процессов. Часто доступ к сети АСУ ТП имеют сторонние, например, сервисные компании или компании производители оборудования, что также чревато проблемами. Зачастую при этом владельцы промышленных объектов уверены в том, что их АСУ ТП изолирована, что не способствует принятию ими мер защиты и предотвращения вторжений.

Если говорить непосредственно о компонентах АСУ ТП, то уязвимыми элементами в них являются ПЛК, сетевое оборудование, промышленные сетевые протоколы общения, а также SCADA-системы. Контроллеры подвержены сетевым атакам вроде DoS/DDoS, часто содержат неизменяемую идентификационную информацию. Используемые сетевые протоколы нередко не имеют механизмов подтверждения аутентификации и шифрования данных. Что касается SCADA, то, как и обычные Windows приложения, они подвержены всем тем же уязвимостям, и это, безусловно, дает злоумышленникам «простор для творчества». На данный момент только в открытых источниках указано около 650 уязвимостей в SCADA-системах, и эта цифра продолжает расти.

В современных условиях информационные системы АСУ ТП должны как содержать защиту от «обычных» зловредов, так и располагать специальными средствами для противодействия целенаправленным атакам.

Текущие трудности

К сожалению, сегодня в России защиту промышленной инфраструктуры затрудняют как архитектурные, так и организационные и технологические факторы. Не способствует решению проблем и сложная бюрократическая процедура внесения изменений в работу промышленных и особенно критически важных промышленных объектов.

Как известно, российские АСУ ТП, однажды пройдя процедуру ввода в эксплуатацию, «опечатываются» и работают без обновлений многие годы. Строгие регламенты и нормативные акты не позволяют вносить в уже сертифицированную систему какие-либо изменения, даже в виде обновления операционной системы. Между тем, когда происходила приемка системы, проверка встроенных свойств безопасности, скорее всего, не проводилась. Да и само понятие безопасности, как правило, до сих пор сводится к ограничению доступа пользователя по паролю, который, опять же, нередко хранится в открытом виде в базе данных самого приложения.

Вычислительное оборудование АСУ ТП тоже, как правило, вводится в эксплуатацию с уже устаревшими прошивками (внутренним исполняемым микрокодом). Однако на сайте производителя всегда доступна свежая прошивка, в которой ряд известных

проблем с информационной безопасностью уже закрыт, но их наличие никто не проверяет даже на этапе развертывания системы — просто потому, что с администраторов этого никто не требует.

С другой стороны, автоматизацией технологических процессов обычно занимаются не сами предприятия-операторы, а сторонние фирмы-подрядчики. Они, в свою очередь, заинтересованы в реализации именно функциональной составляющей, не придавая особого значения информационной безопасности, поскольку ее реализация — довольно трудозатратное занятие. Таким образом, предприятие получает только ту степень защиты от киберугроз, которая требуется действующим законодательством, ни о каких специальных настройках и проверках речь не идет. В конце концов использующееся ПО «падает» или поддается несанкционированному управлению без особых проблем.

Помимо этого, существуют трудности с обнаружением киберугроз из-за отсутствия сетевого мониторинга, а также с необходимостью привлечения сторонних экспертов, в то время как предприятия не горят желанием сообщать об инцидентах. Наконец, проще переустановить, чем разбираться.

Защита возможна

Вопрос информационной безопасности КВО в России давно назрел, и его следует решать комплексно. Государственные органы всерьез озабочены разработкой регламентных документов. Так, сейчас проходит согласование в министерствах проекта федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». ФСТЭК РФ выпустил приказ от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Эта деятельность, несомненно, полезна, но в условиях XXI в. ее недостаточно — регулирование в области IT/OT сегодня реактивно и явно отстает быстро развивающихся технологий. Помимо регламентных документов, должны быть:

- выработаны методологии и практики для построения защищенной инфраструктуры КВО;

- выработаны единые критерии защищенности инфраструктуры КВО, которые должны оперативно дорабатываться и адаптироваться под изменения ландшафта угроз;
- разработаны методы стимулирования и юридической поддержки КВО, которые уже разрабатывают и применяют эффективные меры защиты;
- образовательные программы для работников и управляющих КВО.

Надежную защиту АСУ ТП можно обеспечить только при сотрудничестве государства, самих предприятий, проектных, научных организаций и производителей решений информационной безопасности.

Необходимо выработать методологии и практики для построения защищенной инфраструктуры критически важных объектов, прийти к соглашению по единым критериям защищенности промышленной инфраструктуры, которые должны оперативно дорабатываться и адаптироваться под изменения ландшафта угроз, разработать методы стимулирования и юридической поддержки тех предприятий, которые уже применяют эффективные меры защиты, а также в обязательном порядке проводить образовательные программы для работников и управляющих АСУ ТП.

Государству также необходимо принимать и другие меры, например организовывать регулярные кибертеррористические тренировки, разработать и внедрить единую политику в области обеспечения и контроля поставок оборудования и ПО для АСУ ТП, создать единые стандарты по приемке и сертификации АСУ ТП при вводе их в эксплуатацию, которые включали бы критерии информационной безопасности.

Сегодня в России нет организаций, которые занимались бы мониторингом ситуации с безопасностью АСУ ТП системно, это вне компетенции любого из существующих госорганов. Именно поэтому «Лаборатория Касперского» видит необходимость в создании Национальной российской тестовой лаборатории по исследованию проблем информационной безопасности критически важных объектов. Такой единый центр мог бы на федеральном уровне исследовать как уже известные, так и перспективные подходы по организации защиты АСУ ТП, своевременно обнаруживать проблемы информационной безопасности в используемых программных

и аппаратных средствах, вырабатывать рекомендации по их устранению, информировать соответствующие предприятия, рекомендовать к использованию протестированные программно-аппаратные средства, обладающие высокими показателями устойчивости к кибератаке, и т. д.

Наряду с этим для защиты ИТ-инфраструктур промышленных объектов нужны и принципиально новые методы, технологии и продукты. Многие производители решений информационной безопасности сейчас пытаются внедрять свои обычные, «офисные» продукты в АСУ ТП, однако такой подход может быть использован только в короткой перспективе. В промышленных системах есть своя специфика и нужны продукты, ее учитывающие. Именно поэтому «Лаборатория Касперского» сейчас работает над созданием ряда специальных решений, предназначенных для защиты АСУ ТП от самых разных киберугроз как на уровне сетевых узлов, так и на уровне защиты информационной сети в целом.

В основе разработок «Лаборатории Касперского» лежит безопасная операционная система, над созданием которой компания работает продолжительное время. Она не является заменой для существующих систем, таких как Windows, Linux, MAC OS, которые предназначены для рабочих станций и серверов. Защищенная ОС предназначена для устройств, для которых важно обеспечить высокий уровень информационной безопасности и надежности, например, для PLC-контроллеров, сетевого оборудования или узлов SCADA-систем.

Операционная система, созданная «Лабораторией Касперского», предоставляет программную среду, которая позволяет любому программному компоненту, будь то драйвер, сервис или приложение, выполнять только предварительно декларированную функциональность. Она обеспечивает такой контроль независимо от того, как реализован исполняющийся программный модуль, предоставляя возможность строить доверенные системы из недоверенных компонентов.

Кроме этого, «Лаборатория Касперского» разрабатывает специализированные средства, предназначенные для информационной защиты сетевых узлов под управлением операционных систем семейства Windows. Принципиальное отличие этих средств от широко распространенных средств антивирусной защиты заключается в том, что они используют ресурсы компьютера нормированным

образом, позволяя гарантировать, что основная функциональность программного обеспечения компьютеров в ответственных применениях будет иметь ресурсы для исполнения.

Также «Лаборатория Касперского» разрабатывает средства сетевого мониторинга, которые анализируют копию сетевого трафика, тем самым гарантируя отсутствие влияния на процессы в управляющей сети. Вместе с тем такого рода мониторинг позволяет на ранней стадии определить нехарактерное поведение сетевых устройств, непредусмотренную сетевую активность, целостность сети, изменения в поведении отдельных сетевых узлов, нарушения в потоке управляющей информации технологического процесса. Мониторинг сетевой информации и предупреждения, генерируемые такой системой, позволяют вовремя информировать подготовленный обслуживающий персонал и принимать компенсирующие или иные меры, предупреждающие негативное развитие ситуации.

Проблемы международного взаимодействия и рекомендации для России и мирового сообщества

С учетом ограниченных перспектив международного сотрудничества в сфере обеспечения безопасности КИИ от ИКТ-угроз востребованным видится развитие форматов, которые не обязательно предполагают согласование официальных подходов государств и национальных регуляторов на уровне международной дипломатии и вообще не обязательно предполагают центральную роль государства. В частности, речь идет о необходимости создания и поддержки отраслевых центров обмена информацией (по аналогии с американскими Центрами обмена и анализа информации (ISAC)), повышения квалификации специалистов по ИБ АСУ ТП и КВО в целом, проведении регулярных киберучений как на национальном уровне, так и с подключением внешних партнеров, а также разработке условий государственно-частного партнерства в сфере обеспечения ИБ КВО и других подобных мерах.

В частности, в рамках международного сотрудничества реалистичной задачей могла бы стать попытка выработать базовые рамочные механизмы обмена информацией об угрозах и инцидентах безопасности на объектах КИИ.

Работа по следующим направлениям могла бы дать возможность осуществить конкретные шаги по осуществлению поставленных целей.

1. Начальным шагом может стать закрепление вопросов защиты КИИ от ИКТ-угроз в международной дискуссии. Процесс уже начал развиваться на нескольких площадках в части проблем кибербезопасности объектов мирной атомной отрасли. В продвижение и активизацию широкого публичного обсуждения этих вопросов внесли вклад экспертные исследования и инициативы. В 2013 г. на сайте Госдепартамента США было опубликовано исследование «Кибербезопасность АЭС», выполненное интернациональной группой экспертов из США, Германии и Италии. В числе рекомендаций, сформулированных авторами, Совету Безопасности ООН, в частности, предлагается в рамках главы VII Устава ООН рассмотреть и при необходимости внести поправки в тексты «антитеррористических» резолюций 1373 (2001)[1] и 1540 (2004)[2] с тем, чтобы их положения также распространялись на акты кибертерроризма в отношении ядерных объектов.

В январе 2014 г. доклад о мерах сдерживания и ответственного поведения государств в киберпространстве с упором на снижение рисков для объектов мирной атомной отрасли выпустил Институт «Восток–Запад»[3]. Одна из ключевых рекомендаций доклада призывала государства и частный сектор открыть на площадке Саммита по ядерной безопасности в Гааге дискуссию о выработке предварительного соглашения о том, что кибератаки, нарушающие безопасное функционирование гражданских атомных объектов в мирное время, должны быть запрещены многосторонним юридически обязывающим документом[4].

---

[1] Резолюция 1373 (2001), принятая Советом Безопасности на его 4385-м заседании 28 сентября 2001 г. S/RES/1373 (2001). URL: http://www.un.org/ru/documents/ods.asp?m=S/RES/1373(2001) (дата обращения: 01.03.2016).

[2] Резолюция 1540 (2004), принятая Советом Безопасности на его 4956-м заседании 28 апреля 2004 г. URL: http://www.un.org/ru/documents/ods.asp?m=S/RES/1540(2004) (дата обращения: 01.03.2016).

[3] A Measure of Restraint in Cyberspace Reducing Risk to Civilian Nuclear Assets, East-West Institute, January 2014. URL: http://www.ewi.info/sites/default/files/A%20Measure%20of%20Restraint%20in%20Cyberspace.pdf (дата обращения: 01.03.2016).

[4] Там же, см. с. 19.

Эта рекомендация не была в полной мере учтена в ходе саммита, который состоялся 24–25 марта 2014 г. Однако проблематика кибербезопасности ядерных объектов все же была затронута на его площадке. В итоговом коммюнике саммита этим вопросам уделены два абзаца[1], которые, помимо прочего, призывают государства и частный сектор к разработке более эффективных стратегий снижения рисков атак на АСУ ТП и информационные системы атомных объектов, но не предлагают каких-либо международно-правовых нововведений в этой связи.

Важной вехой стала прошедшая 1–4 июня 2015 г. первая Международная конференция по компьютерной безопасности в ядерном мире, организованная МАГАТЭ. Задача конференции была определена как создание площадки для широкого обмена мнениями по вопросам защиты объектов ядерной отрасли от ИКТ-угроз, а также обсуждения возможностей укрепления роли МАГАТЭ по развитию международного сотрудничества в этой области. Содержание большей части докладов и обсуждений на конференции показало значительный зазор между развитием мысли в рамках экспертного трека 2 и видением проблем кибербезопасности атомной отрасли государствами и межправительственными организациями, включая прежде всего само МАГАТЭ. Правительства куда осторожнее экспертов оценивают перспективы тесного международного сотрудничества и выработки новых механизмов в этой нише; предпочтение отдается более узким, практическим и техническим задачам, для которых идеально подходит площадка МАГАТЭ. Причины лежат на поверхности: атомная отрасль особо чувствительна для национальной безопасности, что сильно ограничивает возможности обмена данными об инцидентах на атомных объектах, а также организации трансграничного содействия в расследовании таких инцидентов.

Вместе с тем формирование постоянной дискуссионной площадки для вопросов кибербезопасности атомной инфраструктуры показывает растущую важность этих вопросов для МАГАТЭ, а также для государств, развивающих мирную атомную энергетику. Поддержка этих треков и участие в них представляется востребованными для России и других государств направлениями

[1] Коммюнике Гаагского саммита по ядерной безопасности. URL: http://www.nss2016.org/2014-communiqu (дата обращения: 01.03.2016).

работы. Вопросы ИКТ-угроз объектам КИИ в отрасли атомной энергетики также были затронуты в рамках IV Международной конференции по вопросам киберпространства, которая состоялась 16–17 апреля 2015 г. в г. Гааге, Нидерланды. Полезным и авторитетным форматом также стал международный научный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности», который ежегодно проходит в г. Гармиш-Партенкирхен, Германия. Наконец, дискуссия о безопасности КИИ атомной отрасли может получить должное развитие и в рамках генеральных конференций МАГАТЭ.

2. Учитывая высокий уровень компетенций МАГАТЭ в сфере разработки рекомендаций и практической проработки вопросов кибербезопасности на объектах ЯТЦ, целесообразным шагом в среднесрочной перспективе может стать закрепление за Агентством центральной роли в развитии и координации международного сотрудничества по борьбе с ИКТ-угрозами КИИ атомной отрасли. В частности, предметом обсуждения могут быть следующие меры:

- Формирование при МАГАТЭ международной базы данных по компьютерным инцидентам на объектах атомной отрасли. Информация, конфиденциально поступающая в подобный «информационный репозиторий» от государств-членов, компаний и экспертов ИБ-сектора и предприятий атомной отрасли, могла бы использоваться для развития рекомендаций и повышения экспертизы Агентства в этой области. Для создания базы данных может быть использован опыт существующих в частном секторе форматов — например, репозитория инцидентов безопасности на промышленных объектах (The Repository of Industrial Security Incidents, RISI).
- Кроме того, в случае успешного развития формата репозитория МАГАТЭ могло бы выполнять функцию связующего звена между компаниями сектора ИБ, командами государственных экспертов и государствами, сталкивающимися с компьютерными атаками на объекты КИИ атомной отрасли и нуждающимися в оперативном содействии для их устранении и расследования. К примеру, в случае со Stuxnet наличие такого механизма позволило бы Ирану оперативно, открыто или конфиденциально, запросить у МАГАТЭ информацию о сходных инцидентах из репозитория, а также сделать запрос на содействие в опе-

ративном устранении и расследовании атаки со стороны самих экспертов МАГАТЭ и, например, России и «Лаборатории Касперского». Добровольный и, по желанию, конфиденциальный характер участия сторон в таком механизме мог бы позволить решить вопросы дефицита доверия. Кроме того, глобальный характер МАГАТЭ обеспечил бы всем государствам-членам доступ к такому механизму, в отличие от RISI и других существующих баз данных.

- Наконец, в среднесрочной перспективе под координацией и на площадке МАГАТЭ с учетом компетенций Агентства могла бы стартовать разработка рамочного соглашения об обеспечении безопасности КИИ в атомной отрасли. Принятие подобного документа, помимо создания для государств стимулов к развитию регулирования данных вопросов, позволило бы в полной мере задействовать лучшие практики и экспертизу, которые могут быть накоплены Агентством в рамках работы механизма репозитория данных об инцидентах на объектах КИИ атомной отрасли. Однако на данном этапе рассматривать конкретное наполнение такого соглашения, как и прогнозировать сроки его возможной разработки и принятия, преждевременно.

3. За рамками МАГАТЭ потенциал имеют и другие форматы наращивания возможностей международного сотрудничества по обеспечению безопасности объектов КИИ от ИКТ-угроз. Однако именно объекты атомной отрасли (возможно, наряду с иными техногенноопасными объектами) имеют наибольшие шансы стать «стартовой площадкой» для международной проработки всей сферы безопасности КИИ. В пользу такой оценки говорит осознание международным сообществом особой опасности таких объектов, их ограниченного и легко идентифицируемого перечня и развитой практики международного регулирования их работы, которая накоплена в том числе усилиями МАГАТЭ.

4. Наряду с этим одна из задач, работа над которой вряд ли может быть выстроена в рамках МАГАТЭ, — это обеспечение взаимопонимания на международном уровне в части классификации КИИ и причисления к ней тех или иных объектов. Такая мера видится необходимым условием развития международного диалога по вопросам предотвращения угроз в этой сфере. Понимание того, какие объекты тот или иной зарубежный партнер относит

к классу КИИ, может стать важной предпосылкой для наработки взаимных мер доверия и предотвращения кризисов, связанных с трансграничными инцидентами в сфере использования ИКТ.

5. Стороны могут задействовать форматы двусторонних и многосторонних консультаций для обмена опытом в части классификации объектов КИИ. Следующим этапом такого взаимодействия может быть формирование совместной системы классификации объектов, относимых к КИИ. В основе работы над формированием списка/классификации может лежать принцип отсечения тех видов/секторов, по которым нет полного консенсуса. Таким образом, к примеру, из 16 секторов КИ, выделяемых в США, 28 секторов в Швейцарии и 50 видов (подклассификация в рамках семи общих типов угроз) в России в общем списке останутся 10–12 категорий, которые встречаются во всех трех национальных классификациях.

6. За конечную цель такой работы может быть принято утверждение единообразного открытого перечня видов объектов КИИ вместе с инструментарием их классификации. Подобный список мог бы быть ограничен объектами КИИ атомной отрасли либо включать в себя КИИ техногенноопасных объектов и другие виды/секторы КИИ. Наличие общего аппарата классификации КИИ может способствовать развитию двусторонних и многосторонних мер доверия по вопросам безопасности в сфере использования ИКТ. В частности, будет обеспечена возможность своевременного предупреждения об атаках, направленных на критические объекты страны-партнера по соглашениям о мерах доверия.

Кроме того, именно наличие единообразного перечня видов КИИ и системы их классификации может послужить отправной точкой для разработки международных соглашений о запрещении атак на те или иные виды объектов в рамках такого перечня. Речь в том числе может идти об упомянутом перспективном рамочном соглашении об обеспечении безопасности КИИ в атомной отрасли на площадке МАГАТЭ.

Представляется целесообразным обеспечить участие в разработке подобных соглашений Группы правительственных экспертов (ГПЭ) ООН по достижениям в области информатизации и телекоммуникаций. Третий состав группы в 2013 г. уже обратился к изучению вопросов безопасности КИИ; планируется продолжение их изучения в рамках четвертого состава группы в 2015 г.

Практический прогресс в решении этих задач видится возможным к 2020 г. при условии, что в его участии будет принимать активное участие Российская Федерация.

Возможные цели в среднесрочной перспективе (до 2020 г.)

1. Составление на международном уровне открытого единообразного перечня видов объектов КИИ и системы их классификации с целью использования для развития форматов мер доверия в сфере использования ИКТ.
2. Разработка рамочного соглашения об обеспечении безопасности КИИ в атомной отрасли (предположительно на площадке МАГАТЭ).

Дополнительная информация

1. Пискунова Н.А. Перспективы международного сотрудничества в области кибербезопасности ядерной энергетики в преддверии саммита по ядерной безопасности в 2014 г. // Электронный бюллетень ПИР-Центра «Пульс кибермира». Октябрь–ноябрь 2013 г. № 6 (6). URL: http://www.pircenter.org/media/content/files/11/13828249110.pdf (дата обращения: 01.03.2016).
2. Bruce W. McConnell, Greg Austin. A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets. East-West Institute. January 31, 2014. URL: http://www.ewi.info/sites/default/files/A%20Measure%20of%20Restraint%20in%20Cyberspace.pdf (дата обращения: 01.03.2016).
3. Rauscher K.F. and Korotkov A.V. Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace. East-West Institute. 03.02.2011. URL: http://www.ewi.info/idea/towards-rules-governing-cyber-conflict-0 (дата обращения: 01.03.2016).

Документы

1. Проект федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (подготовлен ФСБ РФ, текст по состоянию на 8 августа 2013 г.). Сайт «Российской газеты», URL: http://cdnimg.rg.ru/pril/article/83/27/52/zakonoproekt.doc (дата обращения: 01.03.2016).
2. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами

критически важных объектов инфраструктуры Российской Федерации. Утверждены президентом России Д. Медведевым 03.02.2012, № 803. Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/113.html (дата обращения: 01.03.2016).
3. Компьютерная безопасность на ядерных установках. Технические руководящие материалы. Справочное руководство // Серия изданий МАГАТЭ по физической ядерной безопасности. Международное агентство по атомной энергии. МАГАТЭ: Вена-2012. № 17. URL: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527r_web.pdf (дата обращения: 01.03.2016).
4. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. National Institute of Standards and Technology, 12.02.2014. URL: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (дата обращения: 01.03.2016).
5. OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35]. OECD Ministerial Meeting on the Future of the Internet Economy. Seoul, Korea, 17–18 June 2008. OECD Website. URL: http://www.oecd.org/sti/40825404.pdf (дата обращения: 01.03.2016).

Раздел IV

Недопустимы попытки вольных трактовок существующих международно-правовых норм в обоснование по сути агрессивных действий с использованием ИКТ. Если говорить о договорных документах, регламентирующих действия в ходе вооруженных конфликтов, то речь идет о целой отрасли международного права, включающей конвенции, разработанные в конце XIX — начале XX в., в конце 40-х и 70-х гг. минувшего столетия. Все ли правоустановки тех лет вписываются в специфические характеристики киберсферы?

Александр Змеевский,
специальный представитель президента Российской Федерации
по вопросам международного сотрудничества в борьбе
с терроризмом и транснациональной организованной
преступностью

Кибероружие, кибервойны, угрозы, существующие в киберпространстве, должны встретить должное противодействие и быть осуждаемы, запрещаемы и наказуемы. В частности, кибероружие должно быть запрещено для использования в сети Интернет — желательно на уровне ООН. В противном случае все наши сети и устройства станут «питательной средой» для его дальнейшего развития и распространения.

Андрей Ярных,
руководитель стратегических проектов
ЗАО «Лаборатория Касперского»

Использование ИКТ в военно-политических целях: вызовы глобальной безопасности и международному праву

Развитие потенциала использования ИКТ в военно-политических целях

На сегодняшний день можно констатировать, что становление ИКТ в качестве неотъемлемой составляющей национального оборонительного потенциала, военной доктрины и инфраструктуры фактически приняло необратимый характер среди ведущих мировых держав. Эта тенденция проявляется в нескольких направлениях (см. табл. 3).

В настоящее время у технологически развитых государств мира сформирован полноценный финансовый, кадровый, инфраструктурный потенциал для использования ИКТ в военно-политических целях. С учетом эволюции вредоносного ПО, роста угроз критической инфраструктуры и нарастающей зависимости от ИКТ всех ключевых секторов глобальной и национальной экономики, управления и безопасности и других тенденций, рассмотренных в разделах I–IV, возможности достижения целей конфликта при использовании потенциала ИКТ развитыми государствами приближаются к возможностям кинетических вооружений и даже оружия массового уничтожения.

Кроме того, военный ИКТ-потенциал получает доктринальное оформление и закрепление, которое в большинстве случаев не исключает — либо напрямую постулирует — необходимость превентивных операций в информационных сетях. По сути, в отсутствие сдерживающих международно-правовых факторов происходит эрозия негласно устоявшегося после Второй мировой войны и принятия Устава ООН принципа, согласно которому деятельность государств в военно-политической сфере по умолчанию преследует цели и ограничивается задачами обороны.

Результатом является постепенная трансформация ландшафта международной безопасности и переоценка рисков и вызовов в этой сфере всеми членами международного сообщества. Пользуясь асимметричным характером военного потенциала ИКТ, менее

Таблица 3. Развитие военно-политической повестки дня в части использования ИКТ

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
1	**Великобритания**	В сентябре 2013 г. были озвучены планы Минобороны Великобритании по созданию Объединенного резерва кибероборонны (англ. *Joint Cyber Reserve*). Новая структура должна обеспечить поддержку Объединенному подразделению кибероборонны (англ. *Joint Cyber Unit*) в развитии британскими военными полного спектра оперативных возможностей в сфере информационных операций, включая операции превентивного удара. Кроме того, в декабре 2015 г. были анонсированы результаты реализации национальной Стратегии по кибербезопасности, опубликованной в 2011 г. В марте 2014 г. был запущен национальный Центр реагирования на компьютерные инциденты (CERT-UK). В апреле 2014 г. было опубликовано руководство по стандартам кибербезопасности для организаций государственного и частного сектора (*Cyber Essentials*)	В 2013 г. был озвучен план набора в Объединенный резерв кибероборонны нескольких сотен ИТ-специалистов начиная с октября 2013 г. Бюджет создания новой структуры оценивался в 808 млн долл. США. В марте 2015 г. в рамках реализации национальной киберстратегии было анонсировано инвестирование 5 млн фунтов стерлингов в расширение научно-исследовательской деятельности в Центре безопасных информационных технологий (англ. *Centre for Secure Information Technologies, CSIT*) в Белфасте. Предполагается дальнейшее спонсирование профильных вузовских программ	По всей стране расположены 14 кибер-кластеров, осуществляющих НИР, и планируется увеличение их числа

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
2	**Германия**	1. В 2011 г. была принята национальная Стратегия кибербезопасности ФРГ. Приоритетное внимание в стратегии уделяется вопросам обеспечения кибербезопасности бизнеса и общества, борьбе с киберпреступностью. Вопросам кибероборонe в документе отводится сравнительно меньшее внимание, однако военные операции в киберпространстве упоминаются в числе приоритетных угроз. 2. В 2015 г. международные СМИ получили доступ к информации о разработке Министерством обороны ФРГ проекта «Белой книги» под названием «Стратегическое руководство по вопросам кибероборонe» (Strategic Guideline of Cyber Defense). Проект документа отражает ключевые вопросы в сфере обеспечения кибероборонe для германских вооруженных сил на 2016 г. В частности, в проекте «Белой книги» отмечается необходимость развития как оборонительного, так и проактивно-наступательного потенциала для операций в киберпространстве. Также в документе киберпространство рассматривается как самостоятельная «оперативная среда» наряду с сушей, морем, воздушным и космическим пространствами	1. В 2011 г. был создан Национальный центр кибероборонe ФРГ, который объединил ресурсы информационной безопасности и обороны нескольких федеральных органов, включая Вооруженные силы и Федеральный офис информационной безопасности. Задача центра состоит в противодействии ИКТ-атакам на государственные информационные системы ФРГ. 2. В 2012 г. стало известно о наличии при Министерстве обороны ФРГ Подразделения операций в компьютерных сетях (Computer Network Operations Unit), в задачи которого входит формирование потенциала германских вооруженных сил по проведению кибероперaций, а также отработка и симуляция специальных операций в киберпространстве в условиях, приближенных к реальным	

Продолжение таблицы 3

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
3	**КНР**	Несмотря на то что официально принятая доктрина либо стратегия КНР в сфере информационном безопасности отсутствует, большое значение имеют неофициальные экспертные документы, отражающие взгляды вооруженных сил Китая на вопросы операций в киберпространстве и использования ИКТ в военно-политических целях. Один из таких документов — первое с 2001 г. издание публикации «Науки военной стратегии» (The Science of Military Strategy), авторы которой — сотрудники Академии военных наук КНР. В документе вопросам ИКТ отведена отдельная глава, в которой в числе прочего содержатся указания на то, что в структуре НОАК существуют регулярные подразделения для решения задач кибероборонны, а также ведения проактивных операций в киберпространстве. Такие боевые операции в компьютерных сетях включают в себя и поиск уязвимостей и иных данных в сетях потенциального противника. Кроме того, в документе отмечается, что определенные возможности по проведению кибероперациий, помимо НОАК, также закреплены за Министерством государственной безопасности и Министерством общественной безопасности КНР. В целом документ создает довольно резкий контраст с официальным подходом МИД КНР, продвигаемым на международной арене и ставящим во главу угла исключительно мирное использование ИКТ	По данным правительства США и компании Mandiant, в структуре китайской НОАК как минимум с 2006 г. действует так называемое подразделение 61 398 (англ. *Unit 61 398*, также известное как *Advanced Persistent Threat 1*), осуществляющее проактивные операции в информационных сетях других государств, прежде всего США. Штат подразделения составляет до 2000 человек, в его работе задействовано более 1000 серверов. Сообщается также о наличии множества других подразделений, имеющих тесные связи с Министерством обороны КНР, ведущих свою деятельность на постоянной, фактически штатной основе	

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
4	**Россия**	1. В июле 2013 г. были утверждены «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». В документе отводится внимание вопросам использования ИКТ в военно-политических целях и формулируется ряд направлений внешней политики России, преследующих целью нейтрализацию таких угроз. К таким направлениям относится формирование многоуровневой системы международных договоренностей в сфере обеспечения МИБ, а также создание на международном уровне условий для установления международного правового режима нераспространения информационного оружия. 2. С 2015 г. на площадке Совета Безопасности РФ ведется работа по выработке обновленной Доктрины информационной безопасности России, которая в 2016 г. должна быть принята и прийти на смену предыдущей доктрине от 2000 г. Новый документ уделяет первоочередное внимание в том числе вопросам «использования ИКТ в военно-политических целях». В числе приоритетных угроз в проекте новой доктрины отмечается активное наращивание потенциала в сфере ИКТ зарубежными государствами, использование ИКТ государствами и акторами-посредниками «в качестве инструмента для подрыва суверенитета и территориальной целостности» других стран, а также доминирование отдельных государств в информационном пространстве.	1. Осенью 2012 г. был создан государственный Фонд перспективных исследований, задуманный как своеобразный аналог американского Агентства перспективных оборонных исследований (DARPA). Цель Фонда, согласно Федеральному закону от 16.10.2012 № 174-ФЗ «О Фонде перспективных исследований», состоит в содействии прорывным исследованиям и разработкам в интересах безопасности и обороны России. Приоритетные программы и направления работы Фонда включают в себя перспективные системы обработки и передачи информации, разработки в сфере ИИ и когнитивных технологий, кибербезопасность, технологии обнаружения и социальные сети. 2. В 2013–2014 гг. сообщалось о создании в России до конца 2014 г. аналога Киберкомандования США в структуре Генерального Штаба ВС. Предположительно, речь идет о новом роде войск, который на начальном этапе получит статус Главного управления МО России	17 октября 2012 г. Минобороны России объявило конкурс НИР по ряду тем, включая тему «Методы и средства обхода антивирусных систем, средств сетевой защиты, средств защиты ОС», предполагающую разработку ПО для преодоления защитных систем вероятного противника

Продолжение таблицы 3

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
4	**Россия**	С целью ответа на эти и другие угрозы проект доктрины предусматривает развитие в России сил и средства информационного противоборства, а также работу в направлении создания в информационной сфере системы стратегического сдерживания и предотвращения военных конфликтов. 3. На ведомственном уровне проработка проблем кибероборонны и информационной безопасности в контексте боевых действий ведется Минобороны РФ. В 2011 г. был выпущен неофициальный документ «Концептуальные взгляды на деятельность Вооруженных Сил РФ в информационном пространстве», в котором нашли отражение взгляды военных на вопросы информационного противоборства, информационного обеспечения и сопровождения боевых действий и операций ВС РФ		
5	**США**	1. В Международной стратегии для киберпространства США (май 2011 г.) утверждается принцип рассмотрения киберпространства в качестве «пространства оперативных действий ВС США» — т.е. поля боя наряду с водой, воздухом, сушей и космосом. 2. В ноябре 2011 г. Пентагон подтвердил закрепленное в стратегии право использовать «все необходимые средства», включая военные, «для защиты от киберугроз», приравняв кибератаки к вооруженному нападению.	1. 23 июня 2009 г. было сформировано Киберкомандование США (U.S. CYBERCOM), которое объединило ресурсы и подразделения кибер-обороны ВВС, ВМФ и сухопутных войск США (Киберкомандование ВМС США (10-й флот), 24-ю Воздушную армию, Киберкомандование сухопутных войск США и проч.). U.S. CYBERCOM защищает ИКТ-инфраструктуру ВС США, осуществляет операции в киберпространстве, включая наступательные, и подчиняется Стратегическому командованию	1. В августе 2014 г. стало известно о ПО Monstermind, разрабатываемом и используемом АНБ США, но, по сути, выполняющем задачи проактивной обороны в Сети. Функционал программы включает автоматическое распознание и отражение сетевых атак, а также проактивные ответные действия без участия человека — в частности, получение доступа к данным на управляющих серверах, с которых ведется атака, путем преодоления их защиты.

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
		В мировой практике появился прецедент права асимметрично реагировать на ИКТ-угрозы с использованием полного спектра вооружений. 3. В апреле 2015 г. Пентагон опубликовал новое издание Стратегии для киберпространства. В документе нашло отражение ухудшение двусторонних отношений с Россией: была констатирована приостановка диалога США–РФ по вопросам стратегической стабильности в киберпространстве. Вместе с тем отмечается, что подобный формат стратегического диалога продолжает работать в отношении КНР. Кроме того, в стратегии идентифицированы ключевые источники угроз кибербезопасности США на государственном уровне: Китай, Россия, КНДР и Иран. К концептуальным нововведениям стратегии следует отнести упор на проактивные методы, стратегии и технологии операций в киберпространстве. Пентагон сохранил и даже заострил установку на недостаточность усилий исключительно по «пассивной» обороне и обеспечению безопасности ИТ-инфраструктуры. Для успешного решения задач в киберпространстве необходима проактивная деятельность. В документе также сформулированы три стратегические цели Минобороны США в отношении киберпространства: защита собственной информационной сети, укрепление взаимодействия с частным сектором и использование киберпространства для поддержки военных операций США	ВС США в качестве координационного центра операций вооруженных сил с использованием ИКТ. 2. Согласно данным, раскрытым Эдвардом Сноуденом, в 2013 г. на операции АНБ США и других структур, включая U.S. CYBERCOM, в зарубежных информационных сетях было предусмотрено финансирование в объеме 4,3 млрд долл. США. По тем же данным, в 2011 г. была осуществлена 231 проактивная операция, цели которых в том числе включали в себя «предотвращение распространения ядерного оружия». В 2014 г. на нужды Киберкомандования планировалось выделить 447 млн долл. США, в 2,3 раза больше по сравнению бюджетом 2013 г. (191 млн долл. США). Одну из статей расходов должно составить наращивание личного состава структуры до 1800 человек к 2015 г. и до 6000 человек к 2018 г. 3. Совокупные расходы Пентагона на обеспечение кибербезопасности и кибероборонывыросли до 5 млрд долл. США в рамках бюджета на 2015 г. на фоне сокращения многих других расходных статей ведомства	2. Разработка и внедрение на обогатительные иранские объекты ПО Stuxnet рассматривается в качестве элемента обширной программы «Олимпийские игры», которая была в активной фазе как минимум с 2007 по 2012 г. Программа велась с участием специалистов Киберкомандования США, в том числе в части разработки ПО для саботажа стратегических объектов. Составляющими операции «Олимпийские игры» также считаются многие образцы сложного вредоносного ПО, выявленного в странах Ближнего Востока в 2011–2014 гг. (Flame, Mini-Flame, Gauss, DuQu)

Продолжение таблицы 3

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
6	**Франция**	1. В «Белой книге» Министерства обороны Франции (опубликована в апреле 2013 г.) отмечается, что, если информационные атаки ставят под угрозу стратегические национальные интересы Франции, в качестве ответной меры могут быть задействованы любые ресурсы, включая ресурсы Минобороны. В этой связи важной составляющей национальной стратегии кибероборонны являются наступательные действия в киберпространстве, а также разведка. 2. В 2015 г. была принята Национальная стратегия безопасности в цифровом пространстве (Stratégie nationale pour la sécurité du numérique). В документе выделены Стратегические цели, отражающие приоритеты национальной политики в отношении киберпространства и кибербезопасности. В их числе цель № 5: стремление к укреплению стратегической цифровой независимости Европы, а также стратегической стабильности в киберпространстве. Среди путей достижения этой цели выделяется обеспечение глобальной стабильности в киберпространстве за счет международного взаимодействия в наращивании потенциала в сфере кибербезопасности и кибероборонны. Интересно, что авторы стратегии отмечают прогресс ВС США в определении (атрибуции) источников кибератак, что позволяет осуществлять активную оборону и принимать активные контрмеры в отношении агрессоров	В январе 2014 г. министр обороны Франции Жан-Ив Ле Дриан озвучил планы ведомства по запуску программы укрепления национальной кибероборонны стоимостью 2 млрд долл. США. В рамках программы планируется расширить штат подразделения кибероборонны в оборонном ведомстве Франции в два раза — до 450 человек, в том числе за счет запуска с 2015 г. магистерских курсов при Минобороны по специальности Cyber Crisis Management	

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
7	**НАТО**	1. Эффективная кибероборона была включена в число важнейших условий безопасности НАТО в новой Стратегической концепции Альянса от 2010 г. 2. В ходе саммита НАТО 4–5 сентября 2014 г. в Уэльсе, Великобритания, была принята Углубленная доктрина кибероборонны НАТО, которая включает кибератаки в число ключевых угроз безопасности альянса. 3. Также по итогам саммита в Уэльсе участниками в рамках рассмотрения Углубленной доктрины кибербороны было принято заявление, где отмечалось, что нападение на членов НАТО в киберпространстве в отдельных случаях может служить причиной задействования статьи 5 Вашингтонского договора (право применять механизм коллективной обороны, не ограниченной киберпространством)	1. В 2008 г., через год после затяжной волны атак на ИКТ-инфраструктуру Эстонии, недоказанные подозрения в которой пали на Россию, в г. Таллине был основан Объединенный центр передового опыта по кибербороне НАТО (CCD COE). Функции Центра заключаются в экспертной проработке вопросов использования ИКТ в военно-оборонительных целях с международно-правовой и стратегической точек зрения, развитии потенциала и обмене экспертным опытом. 2. Объединенный центр в Таллине действительно аккумулировал ключевые компетенции экспертов стран НАТО в вопросах кибербезопасности и кибербороны. Весной 2013 г. центр опубликовал Таллинское руководство по вопросам применения международного права в условиях конфликта в киберпространстве. Экспертный документ объемом порядка 300 страниц, подготовленный Международной экспертной группой (МЭГ) на площадке центра, стал первой системной попыткой адаптировать и интерпретировать международное гуманитарное право (jus in bello, jus ad bellum) применительно к конфликтам в новой нефизической среде.	Альянс проводит регулярные учения по кибербезопасности и кибероборо-не; впервые такие учения состоялись в январе 2008 г. на базе Таллинского центра CCD COE. Крупнейшие учения «Locked Shields — 2015» прошли в апреле 2015 г. и включали в себя имитацию масштабных трансграничных кибератак на информационную инфраструктуру НАТО со стороны как государств, так и негосударственных акторов. В учениях, которые также были организованы на базе Таллинского центра, приняли участие порядка 400 специалистов из 16 стран НАТО.

Окончание таблицы 3

№	Государство/ МО	Доктринальное и законодательное закрепление использования ИКТ в целях обороны и иных военных целях	Формирование структурно-организационной, финансовой и кадровой базы оборонного потенциала в сфере ИКТ	Развитие государствами технологической базы в целях укрепления военно-оборонительного потенциала в сфере ИКТ
7	**НАТО**		3. С 2013 г. МЭГ ведет работу над Таллинским руководством 2.0. Новый документ должен охватить вопросы интерпретации и применения международного гуманитарного права и других международно-правовых норм «в мирное время», т. е. в ситуациях, не пересекающих порог вооруженного конфликта. Таллинское руководство 2.0 планируется опубликовать в 2016 г. 4. Подготовка кадров для решения задач по поддержке функционирования и обеспечения безопасности информационных систем и коммуникационной инфраструктуры организации осуществляется в том числе на базе Школы коммуникаций и информационных систем (NCISS) НАТО в г. Латина, Италия. В ближайшем будущем планируется передислокация школы в Португалию и расширение ее деятельности с бóльшим упором на подготовку и образование кадров для решения задач в сфере кибероборонны	

развитые государства также постепенно втягиваются в цифровую *гонку вооружений* в надежде получить собственные преимущества в этой сфере и блокировать риски, исходящие от более развитых в области ИКТ держав. По информации спецпредставителя президента России по вопросам международного сотрудничества в области ИБ А.В. Крутских, в 2015 г. более 140 стран мира вели деятельность по созданию «информационного оружия».

Отдельно стоит подчеркнуть нерешенность проблемы идентификации субъектов неправомерных действий с использованием ИКТ и достоверной атрибуции этих действий. Технические сложности атрибуции в условиях развития доктрин активной обороны в ИКТ-среде также могут способствовать развязыванию и эскалации международных конфликтов.

- Атаки на ИКТ-инфраструктуру Эстонии в 2007 г., информационные сети госорганов и частного сектора Грузии в 2008 г., а также на финансовые учреждения и предприятия частного сектора США весной 2014 г. (кампания Energetic Bear, ПО Dragonfly) устойчиво приписываются России рядом государств, включая страны НАТО, в отсутствие надежных технических данных, позволяющих установить такую связь.
- В случае молниеносной сетевой атаки, имитирующей «почерк» русскоязычных злоумышленников (например, производные от кириллицы фрагменты кода), на критическую инфраструктуру стран — членов НАТО с использованием серверов, расположенных на территории России, возникает риск военного ответа НАТО против России. В соответствии с принятой альянсом доктриной ответные меры могут включать использование кинетических вооружений, а также участие в ответном ударе всех стран блока, что в теории влечет риск международного конфликта с участием ядерных государств. Ключевым фактором такого риска является как раз невозможность достоверной атрибуции атак в ИКТ-среде в короткие сроки, которыми принимающие решения лица располагают при угрозе объектам критической инфраструктуры.

Угроза

Развитие международных конфликтов в результате операций в информационных сетях, а также применения кинетических вооружений в ответ на подобные операции уже в среднесрочной перспективе (до 2020 г.).

Проблемы и перспективы адаптации международно-правовой системы в контексте адаптации к военно-политическим вызовам ИКТ

Ключевая проблема нынешней ситуации состоит прежде всего в отсутствии на международном уровне механизмов предупреждения и сдерживания описанных выше конфликтов. Современная система международного права фактически не адаптирована к вызовам и угрозам использования ИКТ в военно-политических целях.

В частности, существуют следующие ключевые проблемы:

- Использование ИКТ в военно-оборонительных целях не охвачено какой-либо системой международных договоров, конвенций и иных соглашений. В качестве условных аналогий следует отметить международные соглашения, которые регулируют вопросы разработки и применения оружия массового уничтожения (Договор о нераспространении ядерного оружия 1967 г., Конвенцию о запрещении химического оружия 1993 г., Конвенцию о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении (КБТО) от 1972 г. и проч.), договоры об ограничении отдельных видов вооружений, Договор о ликвидации ракет средней и меньшей дальности (РСМД) от 1987 г. (серию Договоров о сокращении стратегических наступательных вооружений (СНВ-I, СНВ-II, СНВ-III)), а также соглашения по обычным вооружениям (Договор об обычных вооруженных силах в Европе от 1990 г., Конвенцию о бесчеловечных видах оружия ООН от 1983 г. и проч.).
- Как следствие, отсутствуют международные организации, которые вели бы контроль и мониторинг деятельности государств в части использования ИКТ в военно-политических целях, а также осуществляли верификацию в части соблюдения ограничений в этой сфере. Несмотря на то что идея «МАГАТЭ для киберпространства» неоднократно высказывалась представителями различных организаций и стран (включая главу «Лаборатории Касперского» Е.В. Касперского), пока движение в этой области отсутствует.
- Одной из наиболее острых сторон проблемы является тот факт, что даже существующий корпус норм международного права, регулирующих конфликты и войны вне зависимости от типов

используемого оружия, не может по умолчанию применяться к сфере ИКТ в силу ее технологических особенностей. Речь идет о нормах международного гуманитарного права (*jus in bello*) и права вооруженного конфликта (*jus ad bellum*), которые кодифицированы в таких актах, как Гаагская конвенция 1899 г., Гаагская конвенция 1907 г., Женевская конвенция 1928 г., Женевские конвенции I–IV 1949 г., а также Дополнительные протоколы I–III 1977, 1997 и 2005 гг. к Женевским конвенциям I–IV. Возможность применения указанных документов к вопросам использования ИКТ в военно-политических целях требует единообразной, юридически закрепленной международной интерпретации. Выработка такой интерпретации с учетом отмеченных негативных тенденций в сфере международной безопасности в части наращивания военно-политического потенциала ИКТ видится одним из возможных приоритетов для мирового сообщества на ближайшие годы.

В настоящее время международная дискуссия по этим вопросам развивается в русле двух различных подходов.

Первый подход предполагает признание достаточности существующего корпуса норм международного права (прежде всего *jus in bello* и *jus ad bellum*) для регулирования сферы использования ИКТ в военно-политических целях при условии их адекватной интерпретации и адаптации к специфике ИКТ-среды. Из этой посылки вытекает отсутствие потребности в разработке и принятии каких-либо новых юридически обязательных международных актов, регулирующих данную проблематику.

Этот подход получил развитие в рамках проекта группы экспертов из стран — членов НАТО, проведенный в 2011–2013 гг. на площадке Таллинского центра кибероборонны (CCD COE). Его результатом стало так называемое Таллинское руководство по применению международного права в условиях конфликтов в киберпространстве, опубликованное весной 2013 г. Несмотря на изначально неофициальный характер документа, решения, принятые на саммите НАТО в Уэльсе в 2014 г., фактически следуют некоторым из ключевых выводов авторов документа и, таким образом, означают институционализацию наработок экспертов CCD COE в рамках политики крупнейшего в мире военно-политического блока.

В числе ключевых заключений авторов Таллинского руководства:

- признание ответственности государств за действия акторов-посредников в киберпространстве;
- применимость международно-правового запрета на применение силы к кибероперациям. В отсутствие разработанного определения критерием использования силы признается «нанесение ущерба здоровью людей или повреждение имущества» в результате кибероперации;
- осуществление государством кибероперации в чьих-либо сетях делает это государство легитимной целью для ответных операций в его сетях;
- государство, которое стало жертвой «вооруженного нападения с использованием ИКТ», имеет право ответить применением силы, будь то средства ИКТ или кинетические вооружения. Вооруженным нападением считаются действия, которые повлекли гибель людей или масштабное разрушение имущества;
- конфликт, который разворачивается исключительно в среде ИКТ, при определенных условиях может быть признан вооруженным конфликтом в терминологии международного гуманитарного права (МГП). Соответственно, отдельные категории его участников приобретают статус комбатантов;
- если гражданские лица участвуют в осуществлении кибероперации во время конфликта с использованием ИКТ, они становятся легитимными целями для ответных мер.

Ключевая особенность данного подхода состоит в том, что он не имеет цели запретить использование ИКТ в военно-политических целях, а лишь помогает выработать правила такой деятельности в соответствии с корпусом норм МГП и права вооруженного конфликта.

С 2014 г. экспертами Центра CCD COE готовится второе издание Таллинского руководства, которое планируется опубликовать в 2016 г. Новая версия документа в том числе должна учесть опыт дискуссий вокруг первого издания руководства и дать более четкие ответы на те вопросы, которые авторы документа не смогли разрешить в 2013 г. В числе таких вопросов — возможность применения и адаптации международного гуманитарного права и других международно-правовых норм в условиях мирного вре-

мени. Речь идет о ситуациях, когда кибероперации и другие инциденты с использованием ИКТ не пересекают порога применения силы и тем более вооруженного нападения по смыслу Устава ООН, однако все же могут нуждаться в той или иной международно-правовой квалификации. Один из гипотетических, но реалистичных примеров такого инцидента — кибератака, инициированная государством, актором-посредником или негосударственным актором, которая вызывает критический сбой в работе крупной международной биржи или национальной банковской системы, например за счет необратимого повреждения или удаления электронных данных о совершенных финансовых транзакциях. Человеческие жертвы и физическое разрушение инфраструктуры в этом примере отсутствуют, но экономике пострадавшего государства (или глобальной финансовой системы в целом) может быть нанесен серьезный ущерб. Например, в случае успешной атаки на Нью-Йоркскую фондовую биржу банковская система и экономика США могут потерять многие миллиарды, если не триллионы долларов. Как квалифицировать подобную атаку, наносящую прямой ущерб национальным интересам США? В первом издании Таллинского руководства эксперты пришли к тому, что подобные атаки не могут считаться применением силы по смыслу Устава ООН. Новый документ Таллинского центра НАТО должен дать более подробный ответ на этот и многие другие подобные вопросы. Стоит также отметить, что добровольная политическая норма о ненападении на объекты финансового, в том числе банковского, сектора, в 2014 г. была внесена в повестку обсуждений ГПЭ ООН 4-го созыва по инициативе российских представителей, однако в итоговый доклад группы так и не вошла.

Второй, альтернативный, подход отталкивается от постулата о том, что развитие новой технологической реальности и сферы отношений в рамках ИКТ-среды требует соответствующих новаций в системе международного права, в том числе разработки юридически обязательных международных норм, специально регулирующих эту специфическую сферу в дополнение к уже имеющимся международно-правовым механизмам, включая *jus in bello* и *jus ad bellum*. В качестве возможного решения предлагается принятие глобального договора или конвенции ООН, которые закрепляли бы международный запрет на использование ИКТ в военно-политических целях.

Практическую попытку разработки такого документа предприняла Российская Федерация как основной идеолог и сторонник описываемого подхода. 21–22 сентября 2011 г. на второй международной встрече высоких представителей, курирующих вопросы безопасности, в г. Екатеринбурге Россия представила концепцию конвенции ООН об обеспечении МИБ, вобравшую в себя основные принципы российского подхода, в том числе в части противодействия военно-политическим угрозам в сфере использования ИКТ.

В статье 6 документа перечислены основные меры предотвращения военных конфликтов в информационном пространстве, в число которых входит:

- воздержание от угрозы силой или ее применения против информационного пространства других государств;
- приложение государствами всех возможных усилий для предотвращения использования его территории или инфраструктуры для неправомерных действий с использованием ИКТ;
- отказ от разработки и принятия доктрин, способных спровоцировать возрастание угроз в информационном пространстве и возникновение «информационных войн»;
- принятие мер по ограничению распространения «информационного оружия» и технологий его создания.

Несмотря на то что документ встретил в целом критическую реакцию со стороны западных партнеров России как «претендующий на ограничение прав и свобод в Интернете», изложенные в нем меры остаются ориентиром для России и других сторонников подхода, предполагающего реформирование международного права для нейтрализации угроз в сфере использования ИКТ в военно-политических целях.

Сопоставление этих двух подходов позволяет сформулировать ряд выводов:

- Несмотря на теоретическую возможность выработки корректных интерпретаций норм международного гуманитарного права и права вооруженного конфликта в рамках подхода экспертов НАТО, данный подход не несет предложений по выработке системы международных «сдержек» развязывания и ведения конфликтов в сфере ИКТ. Как уже отмечалось выше, в сфере ИКТ отсутствуют либо только складываются механизмы,

аналогичные тем, что играют роль *страховочной сетки* и дополняют МГП в части сдерживания и предотвращения конфликтов с использованием кинетических вооружений (меры доверия, договоры об ограничении/запрещении отдельных типов оружия, механизмы контроля, мониторинга, верификации, соглашения о разоружении и т. д.). Степень эффективности и достаточности норм МГП в части обеспечения мира и предотвращения конфликтов не может оцениваться без учета этих «специальных» механизмов, так как режим международной безопасности представляет собой комплексную систему. Вследствие этого продвижение и принятие на государственном уровне политики адаптации норм МГП в отсутствие инициатив и норм, «адресно» регулирующих сферу ИКТ, представляется преждевременным и несущим риски для международной безопасности.

- Вместе с тем нормы МГП представляют собой необходимый элемент перспективного режима глобальной безопасности в сфере использования ИКТ. Однако проработка возможностей их корректной адаптации видится целесообразной в рамках не региональных, а глобальных форматов. Опасность параллельной проработки этих вопросов в рамках различных региональных структур и форматов состоит в перспективе появления множественных интерпретаций единых и глобальных норм МГП. Практическим следствием такой коллизии могут стать расходящиеся трактовки сторонами конфликта правомерности действий друг друга, что может повлечь неконтролируемую эскалацию конфликта и его выход за рамки сферы ИКТ.
- Движение вперед в части выработки и принятия глобального юридически обязательного международного документа, направленного на запрещение и предотвращение использования ИКТ в военно-политических целях, видится затруднительным в условиях нерешенной проблемы атрибуции. Обсуждение норм, которые не могут быть подкреплены механизмами верификации, контроля и установления ответственности за их нарушение, может способствовать девальвации идеи такого документа в глазах его потенциальных участников. Однако по мере продвижения в решении проблемы атрибуции задача разработки и принятия подобного документа будет становиться все более актуальной.

Группа правительственных экспертов (ГПЭ) ООН по достижениям в области информатизации и телекоммуникаций

- Основой для формирования группы послужила российская инициатива в сентябре 1998 г., когда глава МИД РФ С.В. Иванов направил Генеральному Секретарю ООН письмо, текст которого включал в себя проект резолюции Генеральной Ассамблеи ООН «Достижения в области в области информатизации и телекоммуникаций». В декабре 1998 г. резолюция была внесена в Первый комитет ГА ООН и принята без голосования (A/RES/53/70). Одним из пунктов текста документа был призыв ко всем странам — членам ООН выразить свои взгляды на вопросы безопасности в сфере ИКТ. С 1998 г. и до настоящего времени одноименные резолюции принимаются ГА ООН ежегодно.
- В декабре 2001 г. Россия выступила с инициативой создания ГПЭ ООН с целью рассмотрения существующих и возможных угроз в сфере ИКТ, возможных мер взаимодействия, а также проведения исследования ключевых вызовов безопасности в этой сфере. Первый состав группы, включавший в себя представителей России, США и еще 13 государств, провел серию встреч в 2004 г. и подготовил формальный доклад (по причине принципиальных разногласий по содержательным вопросам). Тем не менее участники высказали интерес к дальнейшему развитию формата ГПЭ. В результате были также сформированы второй и третий составы ГПЭ, которые провели серии встреч в 2009 и 2013 гг. соответственно. Обе группы согласовали содержательные доклады.
- Четвертый, расширенный состав ГПЭ был сформирован из представителей 20 стран и проводит серию из четырех встреч на основе Резолюции ГА ООН A/RES/68/243, принятой 27 декабря 2013 г. Работа четвертой группы завершилась согласованием и публикацией Доклада от 26 июня 2015 г., в котором наряду с заключениями правительственных экспертов о применении Устава ООН в киберпространстве государствам впервые были предложены добровольные политические нормы ответственного поведения в сфере использования ИКТ.
- В 2016 г. работу продолжит уже пятый состав группы, в задачи которой может войти более глубокая проработка норм ответственного поведения государств и применения основополагающих актов международного права в киберпространстве.

- Решение проблемы атрибуции требует активного взаимодействия представителей государства с техническим сообществом. Учитывая, что львиная доля угроз в сфере ИКТ реализуется через Интернет, целесообразной может быть организация рабочей диалоговой площадки по вопросам атрибуции, которая свела

бы вместе представителей государств и экспертов технических организаций Интернета, включая Рабочую группу по проектированию Интернета (IETF), Совет по архитектуре Интернета (IAB), Руководящую группу по проектированию Интернета (IESG) и проч. Такой опыт стал бы новым шагом в поиске решения проблем атрибуции и способствовал бы привлечению к ее решению более широких кругов специалистов, включая инженеров Глобальной сети.

- Во избежание излишней политизации вопроса о выработке приемлемого подхода к регулированию военно-политической сферы использования ИКТ востребованным представляется перенос дискуссии на нейтральную международную площадку. На данный момент именно такой площадкой является группа правительственных экспертов (ГПЭ) ООН по достижениям в области информатизации и телекоммуникаций, в рамках которой с 2013 г. проработка данных вопросов ведется с участием представителей как России, так и стран НАТО.

Выводы ГПЭ относительно применения норм международного права в сфере использования ИКТ впервые были опубликованы в докладе 2013 г.; в числе их ключевых пунктов:

- международное право, в частности Устав ООН, применимо и необходимо для поддержания мира и безопасности в среде ИКТ;
- государственный суверенитет и вытекающие из него международные нормы и принципы применимы к деятельности с использованием ИКТ, которую ведет государство;
- государства не должны использовать акторов-посредников (англ. *Proxies*) для осуществления международно-противоправных действий, в том числе с использованием ИКТ; государства должны стремиться не допускать использования их территории посредниками с целью противоправного использования ИКТ.

Следующим серьезным шагом вперед стало принятие Доклада от 26 июня 2015 г., в котором подтверждалась применимость Устава ООН в сфере использования ИКТ. Помимо этого, в докладе был сделан ряд новых создающих прецедент выводов по вопросу применимости международного права и использованию ИКТ. Группа признает, что суверенитет государств и проистекающие из него международные нормы и принципы применяются к деятельности

государств, связанной с ИКТ, и к их юрисдикции над информационной инфраструктурой, расположенной на их территориях. В докладе также приведены «неисчерпывающие мнения» его авторов в отношении применимости норм международного права к использованию ИКТ государствами:

- необходимость соблюдения государствами в сфере использования ИКТ таких международно-правовых принципов, как государственный суверенитет, суверенное равенство, разрешение споров мирными средствами и невмешательство во внутренние дела других государств. Применимость существующих обязательств по международному праву к использованию ИКТ государствами, включая обязательства, касающиеся уважения и защиты прав человека и основных свобод;
- признание неотъемлемого права государств принимать меры, соответствующие международному праву и признанные в Уставе ООН;
- упоминание группой существующих принципов международного права, в том числе принципов гуманности, необходимости, пропорциональности и индивидуализации;
- недопустимость использования акторов-посредников («представителей») для совершения международно-противоправных деяний с использованием ИКТ, а также призыв государствам не допускать использования их территории негосударственными субъектами для подобных действий;
- необходимость выполнения государствами их международных обязательств в отношении международно-противоправных деяний при условии того, что обвинения в осуществлении такой деятельности в адрес того или иного государства обоснованны.

Детализированная проработка вопроса об интерпретации ключевых актов международного права, в том числе международного гуманитарного права и права вооруженного конфликта, не входит в задачи и мандат Группы правительственных экспертов ООН. Но работа ее участников, единожды соприкоснувшихся с темой применимости международного права в новой технологической реальности ИКТ, неизбежно будет продолжаться в этом направлении и в дальнейшем. Сделав важный для международного сообщества шаг и вступив на территорию интерпретации фундаментальных международно-правовых понятий, которые

были сформированы 70 лет назад и больше, в новой реальности участники ГПЭ затронули вопрос обновления нынешней системы международного права в новой реальности. ООН как единственный в международном сообществе подлинно глобальный институт в основе своего механизма выработки и принятия решений и норм — Совета Безопасности — до сих пор имеет критерий обладания уникальной технологией — ядерным оружием. Но с течением времени эксклюзивность, уникальность статуса ядерной оружейной державы все больше подвергается вызовам, в основе которых также лежат глобальные технологические перемены. Технологии, в том числе ИКТ, изменили глобальный экономический пейзаж в мире с 1945 г. и таким образом вывели в центр международной политики неядерные государства — Германию, Бразилию, Японию, которых все чаще прочат в новые постоянные члены СБ ООН наряду с «новыми ядерными державами», такими как Индия. Постепенное, ползучее размывание уникальной значимости ядерного статуса происходит и за счет того, что возникают новые формы и факторы силы в международных отношениях, и обладание современными ИКТ относится к числу важнейших из них. Киберпотенциал в исследованиях и заявлениях западных и российских ученых, военных и дипломатов уже неоднократно приравнивался по своей значимости к оружию массового поражения. Уникальность ИКТ заключается в том, что, в отличие от ядерного оружия, этот технологический фактор не сконцентрирован в пространстве и иерархии официальных институтов — он не просто текуч и трансграничен, он противоречит самой концепции вертикально иерархизированного и пространственно ограниченного суверенитета. И это не может не отражаться на материи международного права, определяющей и выстраивающей отношения носителей этого суверенитета — государств. Поиск переходного компромисса, баланса между принципами и понятиями, заложенными в основу международно-правовой конструкции, центром которой во многом остается Устав ООН, и технологически определяемой сетевой реальностью взаимоотношений нового образца, — фундаментальная задача для мирового сообщества, и работа ГПЭ обречена быть ее важной и во многом первопроходческой частью.

Кроме того, выводы и рекомендации ГПЭ относительно применимости Устава ООН так или иначе возвращают внимание

их авторов к важнейшим вопросам понятий, терминологии, которые были поставлены раньше — в момент написания и принятия самого устава. Речь прежде всего идет об определении и соотношении между собой трех фундаментальных понятий — использования силы и ее угрозы, агрессии и вооруженного нападения. Парадокс современности состоит в том, что с момента образования ООН и принятия ее Устава этот вопрос остается не проясненным должным образом.

Поэтому, например, сложность выработки критериев для квалификации использования ИКТ в качестве вооруженного нападения по смыслу Статьи 52 Устава ООН во многом связана с тем, что и вне рамок ИКТ такие критерии не вполне ясны, как и неясны точные критерии отличия использования силы от вооруженного нападения. Таким образом, представители государств и другие эксперты, пытающиеся выработать интерпретации ключевых понятий Устава ООН к использованию ИКТ, параллельно вынуждены решать сложнейшую проблему непроясненности определений, критериев и взаимных отношений самих этих понятий. Какие пути решения этой проблемы могут быть испробованы?

Один из возможных начальных шагов — поиск решений и компромиссных стратегий по интерпретации тех понятий из Устава ООН, для которых конкретные критерии и определения все же существуют — например, понятия агрессии. Хотя Устав ООН не раскрывает понятие агрессии, его подробная интерпретация приведена в Резолюции ГА ООН A/RES/29/3314 от 14.12.1974 «Об определении агрессии». К сожалению, документ, перечисляющий восемь типов действий, которые квалифицируются в качестве агрессии «вне зависимости от факта объявления войны», на момент принятия не мог учитывать действия, связанные с использованием ИКТ.

В результате, когда понятия агрессии и вооруженного нападения используются в доктринальных и иных документах государств и региональных организаций в контексте использования ИКТ, содержание и трактовка этих понятий не могут быть соотнесены с каким-либо общепризнанным источником международного права и остаются плодами интерпретации принимающих их субъектов.

В этой связи востребовано могло бы быть обновление текста резолюции ГА ООН и дополнение его пунктом, который описывает действия с использованием ИКТ, подпадающие под понятие агрессии. Еще одним вариантом могла бы стать выработка консенсусной

интерпретации к использованию ИКТ пункта g упомянутой резолюции ГА ООН № 3314 от 14.12.1974.

Резолюция ГА ООН № 3314 от 14 декабря 1974 г.

Статья 1. Агрессией является применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом Организации Объединенных Наций, как это установлено в настоящем определении.

Статья 3. Любое из следующих действий <...> будет квалифицироваться в качестве акта агрессии:

<...>

g) засылка государством или от имени государства вооруженных банд, групп, иррегулярных сил или наемников, которые осуществляют акты применения вооруженной силы против другого государства, носящие столь серьезный характер, что это равносильно перечисленным выше актам, или его значительное участие в них.

С Резолюцией № 3314 связано еще одно потенциальное направление усиления международно-правового режима ответственности государств за использование ИКТ. Речь идет о расширения юрисдикции Международного уголовного суда на действия с использованием ИКТ, представляющие угрозу международной безопасности, в том числе подпадающие под понятие преступления агрессии.

Право осуществлять юрисдикцию в отношении преступления агрессии было утверждено с принятием Римского статута МУС в 1998 г., однако на сегодня вопрос осуществления данной юрисдикции все еще не решен окончательно. Статья 5 Римского статута МУС перечисляет преступление агрессии в числе преступлений, попадающих под юрисдикцию Международного суда, причем определение агрессии было инкорпорировано в статут из той же Резолюции ГА ООН № 3314, что обеспечивает возможность его расширения за счет определения агрессии с использованием ИКТ в том случае, если соответствующая поправка будет внесена в текст Резолюции ГА ООН.

Тем не менее до сих пор МУС не осуществляет юрисдикцию в отношении агрессии, поскольку все еще не завершил процесс его принятия и инкорпорирования в Римский статут, что является обязательным условием. Разрешение этого вопроса происходит в течение последних нескольких лет — право МУС осуществлять

расследования в отношении преступления агрессии и преследовать подозреваемых в нем было подтверждено на первой Обзорной конференции государств — участников МУС в 2010 г. В то же время было отмечено, что фактическое начало осуществления юрисдикции суда по данному преступлению «зависит от положительного решения Ассамблеи государств — участников МУС, которое может быть принято не ранее 1 января 2017 г.».

Таким образом, фактическое начало осуществления Международным уголовным судом юрисдикции в отношении агрессии произойдет не ранее 2017 г., а возможно, и позже.

Тем не менее задача проработки возможности модификации определения агрессии с учетом использования ИКТ в рамках МУС — параллельно с Резолюцией ГА ООН № 3314 — представляется достаточно актуальной. Несмотря на невысокую практическую отдачу механизмов МУС на данный момент, этот формат имеет свои преимущества:

- в отличие от Резолюции ГА ООН, решения МУС имеют обязательный характер для 122 государств, ратифицировавших Римский статут по состоянию на сентябрь 2015 г.;
- решения МУС и сам факт инициации расследования по подозрению в совершении агрессии с использованием ИКТ может стать серьезным прецедентом, де-факто фиксирующим тот или иной характер действий с использованием ИКТ, квалифицируемых как агрессия.

Возможные цели

1. К 2020–2023 гг.: выработка на площадке ООН согласованного подхода к применению норм существующего международного права (включая нормы международного гуманитарного права и права вооруженного конфликта) в сфере использования ИКТ.
2. Адаптация либо обновление текста Статьи 3 резолюции ГА ООН № 3314 от 14 декабря 1974 г. с целью определения понятия агрессии с использованием ИКТ. Проработка вопроса о расширении компетенции Международного уголовного суда на действия с использованием ИКТ, подпадающие под понятие преступления агрессии.

Но, помимо изложения мнений о применении Устава ООН в сфере использования ИКТ, центральным нововведением Доклада ГПЭ ООН стал перечень добровольных политических норм ответственного поведения в области использования ИКТ, предложенных всему международному сообществу. В числе таких норм:

- необходимость сотрудничества государств в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению угроз международному миру и безопасности, возникающих в связи с использованием ИКТ;
- необходимость тщательного изучения самих инцидентов в сфере ИКТ и их более широкого контекста для того, чтобы надлежащим образом установить, кто несет за них ответственность;
- призыв к государствам заведомо не позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ;
- призыв к государствам отказаться от осуществления или поддержки действий с использованием ИКТ, которые наносят ущерб критически важной инфраструктуре либо так или иначе нарушают ее функционирование;
- принятие государствами мер для обеспечения целостности каналов поставки ИКТ-продукции и борьбы с программными и аппаратными закладками и иным скрытым функционалом в таких продуктах — т. е. программном и аппаратном обеспечении, распространяемом на международных рынках и предназначенном в том числе для объектов критической инфраструктуры;
- добровольный отказ государств от атак на центры реагирования на компьютерные инциденты и аналогичную им инфраструктуру других государств.

На сегодня эти добровольные нормы представляют собой передний край работы международного сообщества по формированию глобального режима ответственного поведения в киберпространстве. Их дальнейшее развитие и детализация возможны в рамках работы уже следующего, пятого созыва ГПЭ ООН, которая запланирована на 2016 г.

Особо интересна норма, нацеленная на запрет и предотвращение деятельности по внедрению программных и аппаратных закладок и иного недекларируемого скрытого функционала в оборудование и программное обеспечение, предназначенное в том числе для обеспечения работы критически важных объектов (КВО). Принятие и добровольное следование этой норме, привлечение к ее исполнению игроков частного сектора, в том числе

компаний в сфере информационной безопасности и международных нишевых сообществ и деловых альянсов, государственно-частных партнерств может стать первым шагом к закладке фундамента действительно работающего режима нераспространения и ограничения создания «кибероружия».

Кроме того, следующим логичным и весьма востребованным для международного сообщества шагом ГПЭ ООН может стать выделение конкретных секторов и отраслей критической инфраструктуры, атаки на которую с использованием ИКТ должны быть запрещены — сначала в формате добровольной нормы, а затем, возможно, и на уровне международно-правового акта. По сути, завершивший свою работу в 2015 г. созыв группы уже начал эту работу, призвав государства отказаться от атак на инфраструктуру центров реагирования на киберинциденты. Кроме того, идея отказа от атак на КИИ банковского и финансового сектора не вошла лишь в нынешний доклад ГПЭ, но скорее всего будет обсуждаться впредь и рано или поздно по ней удастся найти консенсус. Не менее важны вопросы ненападения на инфраструктуру КВО повышенной техногенной опасности, в том числе, как уже отмечалось раньше, объектов мирной атомной энергетики.

Выработка таких договоренностей и особенно их переход из статуса деклараций доброй воли в категорию реально работающих элементов международно-правового режима безопасности в глобальном киберпространстве — долгий, сложный и до сих пор не по всем аспектам очевидный процесс. Одними из главных препятствий на этом пути являются нерешенность проблемы атрибуции противоправных действий с использованием ИКТ, а также трудность создания режима верификации принятых соглашений и взятых государствами обязательств.

Однако постепенное последовательное движение в этом направлении тактикой «малых шагов» является единственным и безальтернативным на сегодня вариантом. Роль ГПЭ ООН в этом процессе исключительно важна, и уже поэтому формат и результаты работы группы нуждаются во всемирной поддержке и продвижении на международном уровне. Вместе с тем формату ГПЭ попрежнему есть куда развиваться. Включение неправительственных экспертов в рабочий формат группы в том или ином статусе позволит существенно усилить качество дискуссий, расширить взгляд на проблемы и артикулировать интересы не только самих

государств, но и других заинтересованных сторон, включая частный сектор, на будущее международно-правового режима ответственного поведения в сфере использования ИКТ.

Дополнительная информация

1. Сондерс Д. Как избежать эскалации конфликтов в киберпространстве? // Индекс безопасности. Весна 2013. № 1 (104). С. 11–16.
2. Война в киберпространстве: уроки и выводы для России. Круглый стол в редакции «Независимого военного обозрения» // Независимое военное обозрение. 13.12.2013. № 46.
3. Черненко Е. Виртуальный фронт // Коммерсантъ Власть. 27.05.2013. № 20 (1025).
4. Интервью члена Военно-промышленной комиссии при Правительстве России Олега Мартьянова и заместителя директора ФПИ Игоря Денисова радиостанции «Эхо Москвы». 02.09.2014. URL: http://www.fpi.gov.ru/press/media/intervyyu_chlena_boenno_promishlennoy_komissii_pri_pravitelystve_rf_olega_martyyanova_i_zamestitelya_direktora_fpi_igorya_denisova_radiostantsii_jeho_moskvi (дата обращения: 01.03.2016).
5. Kodar Erki. Applying the Law of Armed Conflict to Cyber Attacks: from the Martens Clause to Additional Protocol I. ENDC Proceedings, Volume 15, 2012, pp. 107–132.

Документы

1. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. Administration of the President of the United States. May 2011. URL: https://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (дата обращения: 01.03.2016).
2. Tallinn Manual on the International Law Applicable to Cyber Warfare. NATO Cooperative Cyber Defence Centre of Excellence, 2013. URL: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=0/1803379 (дата обращения: 01.03.2016).
3. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. Министерство обороны Российской Федерации, 2012 г. URL: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (дата обращения: 01.03.2016).

4. Доклад Специального докладчика по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях Кристофа Хейнса. Генеральная Ассамблея ООН. A/HRC/23/47. 09.04.2013. URL: http://www.un.org/Docs/journal/asp/ws.asp?m=A/HRC/23/47 (дата обращения: 01.03.2016).
5. Определение агрессии. Утверждено резолюцией Генеральной Ассамблеи ООН 3314 (XXIX) от 14.12.1974. Официальный сайт Организации Объединенных Наций. URL: http://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml (дата обращения: 01.03.2016).
6. Римский статут Международного уголовного суда. Текст Римского статута, распространенного в качестве документа A/CONF.183/9 от 17.07.1998 с изменениями на основе протоколов от 10.11.1998, 12.07.1999, 30.11.1999, 08.05.2000, 17.01.2001, 16.01.2002. Статут вступил в силу 1 июля 2002 г. Международный уголовный суд. Официальный веб-сайт Организации Объединенных Наций. URL: http://www.un.org/ru/law/icc/rome_statute(r).pdf (дата обращения: 01.03.2016).
7. Женевские конвенции и протоколы к ним. Организация Объединенных Наций и международное право. URL: http://www.un.org/ru/humanitarian/law/geneva.shtml (дата обращения: 01.03.2016).
8. Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Записка Генерального секретаря A/70/174. 22 июля 2015 г. Генеральная Ассамблея, Организация Объединенных Наций. URL: http://undocs.org/A/70/174 (дата обращения: 01.03.2016).

Раздел V

Мы признаем, что управление использованием Интернета — это не только присвоение наименований и адресов Интернета. Оно включает и другие существенные вопросы государственной политики, например, такие как основные ресурсы Интернета, безопасность и защищенность Интернета, а также аспекты и вопросы развития, касающиеся использования Интернета.

Тунисская программа информационного общества
от 15.11.2005, параграф 58.

Глобальное управление Интернетом: международно-правовые и международно-политические аспекты

Глобальная архитектура управления Интернетом на современном этапе

На сегодняшний день продолжается активное развитие системы управления Интернетом, которая в своих основных функциональных, структурных и институциональных аспектах сложилась в 1990–2000-х гг. С технической точки зрения развитие архитектуры Интернета и управление Сетью по-прежнему осуществляется в рамках ряда базовых принципов, перечисленных в RFC 1958 (так называемые архитектурные принципы Интернета).

Архитектурные принципы Интернета (RFC 1958, июнь 1996 г.)

- Принцип функциональной совместимости.
- Принцип открытости.
- Принцип сквозной связи (e2e).
- Принцип отсутствия централизованного контроля.

В функциональном плане управление Сетью обеспечивается различными участниками, состав которых также различается в зависимости от охвата их деятельности (глобальный, региональный, национальный и локальный). На сегодняшний день центральную роль в управлении Глобальной сетью играет обусловленная историческими обстоятельствами ее развития модель, известная как управление с участием всех заинтересованных сторон (англ. *multistakeholder Internet governance*).

Управление Интернетом с участием всех заинтересованных сторон

Понятие: управление Интернетом с участием всех заинтересованных сторон (приблизительный перевод с англ. *multistakeholder Internet governance*).

Оформление и закрепление в международной практике:

- Женевский (2003) и Тунисский (2005) этапы Всемирной встречи на высшем уровне по вопросам развития информационного общества (ВВУИО) (проведены в соответствии с резолюцией 56/183 ГА ООН).
- Выводы Рабочей группы по управлению Интернетом при Генеральном секретаре ООН (создана в 2004 г. в преддверии Тунисского этапа ВВУИО, включала экспертов из более чем 40 стран).

Ключевые заинтересованные стороны:

- правительства;
- частный сектор;
- институты гражданского общества (в том числе неправительственные и некоммерческие организации, включая объединения пользователей Интернета);
- де-факто включены позднее: представители научно-образовательного сообщества (англ. *Academia*);
- представители глобального сообщества интернет-пользователей.

Механизм принятий решений: отсутствие приоритета государств в формулировании и принятии решений с учетом позиций всех заинтересованных сторон в равном статусе и порядке.

Развитие международных подходов к управлению Интернетом в русле этой модели закрепляет первоочередную роль различных организаций технического сообщества, которое оформилось еще на самых ранних стадиях развития Сети в 1980–1990-х гг. Основными участниками глобального процесса управления Интернетом на сегодня являются структуры, перечисленные в таблице 4.

Таким образом, ключевые разработки и решения, касающиеся архитектуры Сети, согласовываются, принимаются и воплощаются техническим сообществом, не привязанным к какому-либо международно-правовому режиму осуществления такой деятельности. Более того, некоторые рабочие процессы в этой сфере (такие как деятельность IETF) вообще не опираются на организационные формы, которые бы подпадали под какую-либо национальную юрисдикцию.

Вместе с тем государства и межгосударственные организации также принимают участие в проработке вопросов управления Интернетом. Такая работа в основном ведется в рамках организаций и площадок, встроенных в систему институтов ООН.

Таблица 4. Основные технические организации глобального интернет-сообщества

№	Структура	Описание и функции в сфере управления Интернетом	Статус
1	**Общество Интернета (ISOC)**	Основная организационно-правовая форма, на которую опирается рабочий процесс Рабочей группы по проектированию Интернета (IETF), в рамках которого решаются вопросы стандартизации функционирования Интернета. Под эгидой Общества Интернета в рамках IETF и других рабочих процессов внутри технического сообщества осуществляется содействие открытой разработке стандартов, протоколов администрирования и технической инфраструктуры Сети. Также содействует развитию национальной и международной политики с целью поддержки роста и совершенствования Глобальной сети во всем мире. Под эгидой Общества Интернета действуют: Рабочая группа по проектированию Интернета (IETF); Совет по архитектуре Интернета (IAB); Рабочая группа по интернет-исследованиям (IRTF); Руководящая группа по проектированию Интернета (IESG); Руководящая группа по интернет-исследованиям (IRSG); Редактор запросов на комментарии и предложения (редактор RFC)	Некоммерческая корпорация, юридическое лицо Федерального округа Колумбия, США. Организационная структура построена по принципу членства, деятельность финансируется в основном из взносов юридических и физических лиц. Обладает правами на все документы RFC
2	**Совет по архитектуре Интернета (IAB)**	Действует под эгидой Общества Интернета (ISOC). По поручению ISOC курирует вопросы, связанные с архитектурой Сети, включая протоколы и другие стандарты. Консультирует попечительский совет ISOC по вопросам, связанным с архитектурой Интернета. Также выступает в качестве технического органа по внешним связям от имени ISOC. Также осуществляет координацию деятельности ряда рабочих групп (IETF; а также Рабочая группа по исследованию Интернета, IRTF). Одновременно выступает в качестве Комитета IETF по техническим вопросам	Не имеет юридического лица, является технической координационной площадкой (комитетом)
3	**Рабочая группа по проектированию Интернета (IETF)**	Занимается проектированием и архитектурой Интернета и является основным рабочим процессом, в рамках которого непосредственно разрабатываются, испытываются и внедряются новые технологические стандарты Сети, включая интернет-протоколы. Действует под эгидой ISOC. В IETF вырабатываются не только технические RFC, но и информационные сообщения и продукты типа протоколов совещаний и фиксации бизнес-процессов.	Не имеет юридического лица и организационного статуса, а также штаб-квартиры. Проводит встречи и ведет работу в рамках более чем 120 рабочих групп (списков рассылки).

Продолжение таблицы 4

№	Структура	Описание и функции в сфере управления Интернетом	Статус
		В частности, осуществляет следующие функции: • разработка спецификаций, стандартов и соглашений по общим архитектурным принципам протоколов Сети; • принятие рекомендаций по стандартизации протоколов и вынос их на рассмотрение IESG; • содействие широкому распространению технологий и стандартов, разрабатываемых в Исследовательской группе интернет-технологий (IRTF)	Рабочий процесс IETF построен на волонтерских принципах, за отдельными точечными исключениями
4	**Корпорация Интернета по присвоению имен и номеров (ICANN)**	Осуществляет управление двумя централизованными уровнями инфраструктуры Интернета — уровнями глобальных идентификаторов Сети (глобальная система доменных имен и система IP-адресации). В частности, осуществляет распределение стеков IP-адресов между Региональными интернет-регистратурами (RIRs), которые затем распределяют адреса между операторами и бизнес-потребителями, и делегирование доменных имен верхнего уровня (TLDs). В рамках своего департамента — IANA — осуществляет поддержку и администрирование системы DNS. Предоставляет площадку и является формальным учредителем Координационного комитета операторов корневых серверов DNS	Некоммерческая корпорация, зарегистрирована в штате Калифорния, США. Связана несколькими соглашениями и контрактами с Министерством торговли США
5	**Администрация адресного пространства Интернет (IANA)**	Осуществляет исполнение критических функций системы DNS («функции IANA»), в том числе: • регистрацию технических параметров интернет-протоколов; • администрирование файла корневой зоны системы DNS; • распределение адресных ресурсов Интернета — доменных имен верхнего уровня (TLDs) и стеков IP-адресов; • управление доменом верхнего уровня .arpa в рамках обеспечения работы системы DNS	Не имеет юридического лица, является департаментом в структуре ICANN
6	**Консорциум Всемирной сети (W3C)**	Консорциумом ведутся разработка, оптимизация и содействие внедрению стандартов интернет-протоколов; фактически он выполняет функцию организации по стандартизации по вопросам протоколов Интернета	Некоммерческая ассоциация, не имеет юридического лица. Учрежден совместно лабораторией Массачусетского технологического института (CSAIL MIT и Европейским

Окончание таблицы 4

№	Структура	Описание и функции в сфере управления Интернетом	Статус
			исследовательским консорциумом по информатике и математике (ERCIM)
7	**Региональные регистратуры Интернета (RIR)**	Региональные членские организации, вместе составляющие Систему регистрации номеров Интернета (Internet Number Registry System), описанную в RFC 7020. Статус Региональной регистратуры Интернета присваивается ICANN. Вот уже порядка 20 лет являются важными участниками процесса управления Интернетом. Основные функции региональных регистратур связаны с системой ресурсов нумерации Интернета, включая распределение диапазонов (стеков) IP-адресов и номеров автономных систем (AC), выделяемых ICANN в рамках осуществления функций IANA, поддержку внедрения IPv6 и обеспечения его совместимости с IPv4, регистрацию обратных зон DNS. В побочные функции Региональных регистратур также может входить статистический анализ сетей, мониторинг точек обмена трафиком (Internet Exchange Points), а также поддержка корневых зон DNS. На сегодняшний день существуют пять региональных регистратур, в сумме охватывающих практически все страны мира: 1) American Registry for Internet Numbers (ARIN) — для Северной Америки; 2) RIPE Network Coordination Centre (RIPE NCC) — для Европы, Ближнего Востока и Центральной Азии; 3) Asia-Pacific Network Information Centre (APNIC) — для Азии и Тихоокеанского региона; 4) Latin American and Caribbean Internet Addresses Registry (LACNIC) — для Латинской Америки и Карибского региона; 5) African Network Information Centre (AfriNIC) — для Африки. Регистратура, отвечающая за Европу, Ближний Восток и частично Центральную Азию — RIPE NCC (Réseaux IP Européens Network Coordination Centre). Подробно географическое распределение RIR см. на рисунке 7	Пять региональных регистратур имеют несколько различные правовые формы и статусы, однако во всех случаях речь идет о том или ином варианте неинкорпорированной и некоммерческой членской организации/ассоциации. RIPE NCC представляет собой независимую, некоммерческую членскую организацию, зарегистрированную в Амстердаме, Нидерланды. Членами организации в основной являются интернет-провайдеры из стран представляемого региона. Вместе 5 RIR образуют Организацию ресурсов нумерации (англ. *Number Resource Organization, NRO*), образованную 24 ноября 2003 г. для представления интересов RIR, а также для осуществления между регистратурами совместной деятельности, технических проектов и координации политик

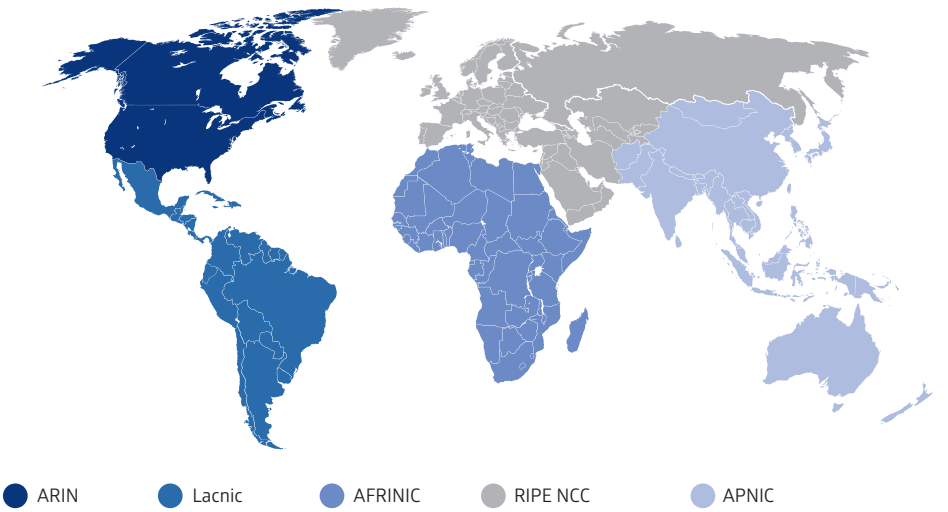


Рис. 7. Карта Региональных регистратур Интернета (RIR) по состоянию на 30 апреля 2015 г.

Источник: The Number Resource Organization

1. Исходным и ключевым из таких форматов является упомянутый механизм ВВУИО, который не прекратил свою работу с окончанием Тунисского этапа в 2005 г. В настоящий момент ведется работа в рамках процесса ВВУИО+10, ключевым этапом которого должна была стать новая всемирная встреча на высшем уровне. Подготовительный процесс к организации встречи продолжался в 2015 г. и завершился встречей высокого уровня на площадке Генеральной Ассамблеи ООН 15–16 декабря 2015 г. в Нью-Йорке, США. Это мероприятие не было собственно новой всемирной встречей, хотя и проходило в рамках заседания ГА ООН. По сути дела, такой формат стал компромиссом, призванным решить хотя бы какие-то вопросы в рамках процесса ВВУИО+10, притом что созвать новый всемирный саммит в 2015 г. не удалось. Саммит в Нью-Йорке призван подвести итог деятельности международного сообщества по развитию Глобальной сети и управлению ей за прошедшее десятилетие.

2. Одним из механизмов, созданных во исполнение решений Тунисского этапа ВВУИО, является Форум по вопросам управления Интернетом (IGF), который был учрежден под эгидой ООН в качестве всемирной площадки для ведения многостороннего политического диалога с участием всех заинтересованных сто-

рон. Мандат форума предусматривал пятилетний срок его деятельности с возможностью последующего продления. В первый раз эта опция была использована в 2010 г., форум получил мандат до 2015 г. Но принципиальные вопросы статуса форума, силы его решений и необходимости бессрочного или хотя бы более длительного закрепления его мандата не были решены. Несмотря на то что в 2015 г. новая всемирная встреча так и не состоялась, по некоторым из этих вопросов интернет-сообществу все же удалось продвинуться вперед. В рамках Встречи высокого уровня в Нью-Йорке в декабре 2015 г. Генеральная Ассамблея ООН приняла решение продлить мандат форума еще на 10 лет — до 2025 г. Для форума, поддерживающего сам механизм и формат ВВУИО, такое решение стало тактической победой — ведь в преддверии нью-йоркской встречи высказывались разные мнения, в том числе призывающие вообще не продлять мандат и распустить форум как структуру, не принимающую обязывающих решений. Действительно, на данный момент форум не является площадкой для выработки международных документов, не выполняет надзорные функции и не вмешивается в вопросы повседневной эксплуатации и технического обслуживания Интернета. Основным форматом его деятельности остаются ежегодные встречи, последняя из которых прошла 10–13 ноября 2015 г. в г. Жоао-Пессоа, Бразилия.

3. Определенный спектр функций, связанных с управлением Сетью, выполняет МСЭ. В конце 1980-х гг. и начале 1990-х гг. деятельность МСЭ по либерализации ценообразования и услуг в сфере коммуникаций внесла весомый вклад в быстрое развитие Интернета. Агентство ООН также принимало активное участие в Женевском и Тунисском этапах ВВУИО. Кроме того, в настоящее время МСЭ рассматривается рядом государств, и прежде всего Россией, как оптимальная площадка для создания всемирной межправительственной организации по вопросам технического управления Интернетом.

4. Отдельные вопросы в сфере управления Интернетом также прорабатывает Всемирная организация интеллектуальной собственности (ВОИС). Организация активно участвует в выработке подходов и стандартов к защите интеллектуальной собственности в Сети, а также взаимодействует с ICANN и региональными регистратурами (RIR) в части разрешения конфликтов вокруг доменных имен.

5. Вопросы управления Интернетом сегодня также включаются в повестку дня большого числа региональных организаций и диалоговых площадок. В их числе Организация экономического сотрудничества и развития (ОЭСР), Совет Европы, «Большая двадцатка» (G20) и остановившая работу с Россией «Большая семерка» (G7) и проч. С 2015 г. в проработку вопросов глобальной цифровой экономики и управления Интернетом очень активно включился Всемирный экономический форум, выпустивший ряд докладов на различные темы — от будущего цифровых финансов до исследования глобальных рисков фрагментации Интернета.

Трансформация подходов в сфере управления Сетью: глобализация vs интернационализация

За последние 10–15 лет сложившаяся *гибридная* система управления Интернетом в целом доказала свою гибкость, эффективность и работоспособность. Но сегодня глобальная архитектура управления Сетью оказывается подвержена магистральным процессам трансформации, которые во многом обусловлены стремлением различных ее участников к пересмотру сложившейся модели и своего места в ней.

За прошедшие с Тунисского этапа ВВУИО годы рост Интернета, разрастание его инфраструктуры и ее усложнение, а также огромный скачок капитализации интернет-сектора стимулировали и способствовали расширению технического сообщества, укреплению его позиций, углублению и расширению его задач. Уникальная практика многолетней работы в условиях относительной свободы принятия решений и — до недавнего времени — крайне ограниченного вмешательства государства в этот процесс привела к тому, что организации технического сообщества сформировали собственное комплексное видение повестки дня в сфере управления Интернетом. Несмотря на преимущественно техническое наполнение этого видения, с каждым годом все более четко обозначается запрос на участие технического сообщества в формулировании глобальных политик развития Сети, в том числе по вопросам, выходящим за рамки сугубо технической плоскости.

По мере развития Глобальной сети некоторые вопросы, ранее имевшие сугубо прикладное значение, объективно приобретают новые грани и измерения, в том числе лежащие в политико-правовой плоскости.

Одним из примеров является развитие глобального доменного пространства, и в частности запуск ICANN программы новых доменных имен верхнего уровня (nGTLDs), прием заявок на которые открылся в июне 2011 г. В ходе реализации программы Корпорации Интернета пришлось разрешать коллизии, связанные с так называемыми *географическими* доменами — например, доменом .amazon, на который подала заявку одноименная компания из США. Заявка была отклонена под давлением сразу нескольких государств Южной Америки, усмотревших в ней нарушение их *естественного права* на обладание этим доменом. До nGTLDs международные споры возникали вокруг домена .xxx для порноконтента (против делегирования которого возражал Консультативный правительственный комитет ICANN — GAC) и еще в ряде случаев. Так или иначе во многих подобных случаях Корпорации Интернета приходилось прорабатывать вопросы, имеющие социальную, политическую, культурную и, конечно, экономическую значимость.

Другим фактором, привносящим в повестку дня ICANN международно-политические аспекты, является длительный процесс трансформации ее отношений с правительством США. Условием создания ICANN в 1998 г. было последующее самоустранение Министерства торговли США от контроля над корпорацией и, в перспективе, завершение контрактных отношений с ней. Этот процесс не завершен до сих пор, хотя во второй половине 2013 г. он получил новый импульс. Серьезный удар по имиджу США как основного защитника Интернета в качестве свободного и открытого пространства, который нанесли разоблачения Сноудена, и возникший вакуум морального лидерства в этой сфере послужили катализатором для переоценки ICANN своих задач и приоритетов. Корпорация осознала, что накопленный ею потенциал лидерства среди структур интернет-сообщества требует скорейшей реализации.

В результате Корпорация Интернета к настоящему моменту взяла на себя роль главной площадки артикулирования интересов по вопросам управления Сетью не только технического сообщества, но и по сути всех заинтересованных сторон. В рамках структуры корпорации были созданы площадки для агрегирования и выражения интересов как представителей самих интернет-пользователей (At-Large), так и правительств (Правительственный консультативный комитет, GAC).

Немаловажным условием, которое позволяет ICANN играть такую роль, является значительное расширение ее финансовых ресурсов, во многом обусловленное развитием программы новых доменных имен верхнего уровня (nGTLDs). Так, по итогам финансового 2014 г. общие доходы ICANN превысили 200 млн долл. США, что означает более чем трехкратный рост по сравнению с показателями пятилетней давности (2009). Опираясь на возросшие ресурсы и лидерство в техническом сообществе, с 2012 г. Корпорация Интернета также реализует программу Глобального взаимодействия с заинтересованными сторонами (англ. *Global Stakeholder Engagement*), а также программу глобализации функций IANA.

Вместе с тем Корпорация Интернета по-прежнему находится в сложном переходном периоде. Ситуация по передаче ответственного управления функциями IANA остается нерешенной. 30 сентября 2015 г. истек очередной контракт на исполнение функций IANA с NTIA, а незадолго до того Департамент торговли использовал один из опционов на его продление — до 30 сентября 2016 г. На конференции ICANN в Буэнос-Айресе в июне 2015 г. было подтверждено, что процесс передачи ответственного управления функциями IANA должен завершиться осенью 2016 г. Дальнейшее продление контракта NTIA с ICANN не предполагается. В марте 2016 г. с публикацией итогового Предложения ICG стала ясна новая конфигурация участников управления уникальными идентификаторами. Определились новые стороны контракта: постпереходная IANA и сама ICANN (вместо правительства США). Но пока не ясно, когда, как и кому будет передано управление бизнес-процессом технического менеджмента корневой зоны DNS. Сейчас его по контракту с NTIA выполняет компания VeriSign, которая генерирует на скрытом мастер-сервере и рассылает по остальным корневым серверам файл корневой зоны, содержащий информацию о доменах верхнего уровня (gTLDs и ccTLDs). Неясный исход, сложность и не всегда очевидная прозрачность процесса провоцируют среди некоторых его участников скептицизм. Одна из главных проблем, в том числе присущая российским официальным представителям и значительной части интернет-сообщества, — глубоко укорененные сомнения в том, что новые структуры технического сообщества, которые будут контролировать выполнение функций IANA вместо Департамента торговли США к концу 2016 г., будут существовать

вне юрисдикции США и получат реальную независимость от американского правительства.

В рамках деятельности, ориентированной на глобализацию своего присутствия и отдельных функций, ICANN:

- в октябре 2013 г. объявила о намерении вывести исполнение критических функций Интернета из-под контроля правительства США, этот сюжет получил развитие в марте 2014 г. (см. раздел VI);
- приступила к расширению присутствия на региональном уровне, открыв сеть региональных офисов и хабов. В апреле 2013 г. был открыт региональный офис в Стамбуле, который также рассматривался в качестве возможного нового головного офиса ICANN. Тогда же было объявлено о планах по открытию

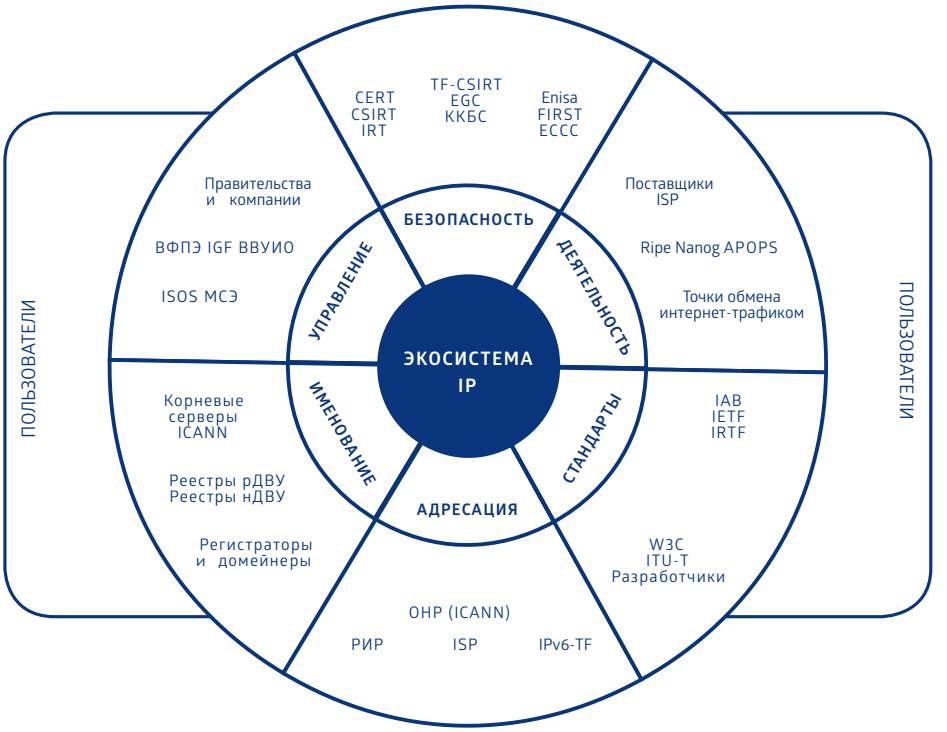


Рис. 8. Экосистема управления Интернетом и место в ней ICANN

Источник: ICANN

региональных офисов и центров взаимодействия с заинтересованными сторонами в Сингапуре и в Пекине;

- взяла курс на наращивание взаимодействия с международными организациями. В феврале 2014 г. было анонсировано открытие офиса в Женеве — «столице» международных организаций, включая ВОИС, МСЭ и другие структуры ООН, а также ВЭФ. В настоящее время вице-президент ICANN по глобальному взаимодействию с заинтересованными сторонами фактически выполняет функции представителя ICANN при международных организациях в офисе корпорации в Нью-Йорке, открытом в 2013 г. В задачи главы офиса входит взаимодействие с ООН, ее агентствами и постоянными представительствами при штаб-квартире организации;
- избрала стратегическим приоритетом укрепление своей международной легитимности, в том числе в институциональном плане. 17 февраля 2014 г. правлением ICANN была утверждена резолюция, инициировавшая создание ряда консультативных групп по глобализации при президенте корпорации (President's Globalization Advisory Groups). В задачи Консультативной группы по правовому режиму (Legal Structure) входит «создание вспомогательной параллельной международной структуры с целью укрепления глобальной легитимности ICANN».

Следствием этих процессов является то, что ICANN при поддержке других представителей интернет-сообщества начинает самостоятельно формировать повестку дня в сфере глобального управления Интернетом, не особенно оглядываясь на традиционные межправительственные механизмы.

Примером является трек NETmundial, импульс к развитию которого дали разоблаченные Эдвардом Сноуденом эпизоды слежки АНБ за президентом Бразилии Дилмой Руссеф. По итогам встречи главы ICANN Фади Шехаде с г-жой Руссеф 9 октября 2013 г. стороны договорились организовать и провести глобальную встречу по вопросам будущего управления Интернетом с участием всех заинтересованных сторон. Целью этой инициативы называлось принятие свода принципов управления Интернетом, выражающих волю заинтересованных сторон и в том числе ограничивающих подобную программам АНБ деятельность государств в Интернете.

Саммит NETmundial состоялся 23–24 апреля 2014 г. в г. Сан-Паулу, Бразилия с участием более 1500 человек. В ходе встречи было выработано и принято итоговое заявление заинтересованных сторон, которое включало в себя принципы управления Интернетом, а также дорожную карту для будущего развития экосистемы управления Интернетом.

Принятые документы подтверждают принцип участия всех заинтересованных сторон, а также предлагают принципы, связанные с безопасностью, культурным и языковым разнообразием, действием прав человека, поощрением инноваций и в Интернете. В рамках дорожной карты обозначен перечень предложений по таким вопросам, как усиление механизма и площадки IGF, передача контроля над исполнением функций IANA интернет-сообществу, усиление многостороннего сотрудничества в сфере кибербезопасности и юриспруденции в Сети и проч.

Встреча в Сан-Паулу создала значимый прецедент: площадка, не имеющая межправительственного статуса, при ведущей роли организации технического сообщества (ICANN) произвела документ, охватывающий ключевые вопросы глобального управления Интернетом в институциональной, социокультурной, экономической и иных сферах. Более того, решения NETmundial предлагается взять за основу дальнейшего развития глобальной дискуссии с участием всех заинтересованных сторон по вопросам управления Сетью. С июля 2014 г. к дальнейшему развитию Инициативы NETmundial подключился Всемирный экономический форум (ВЭФ). Таким образом, интернет-сообщество приступило к формированию и реализации глобальной повестки дня по всему спектру вопросов управления Интернетом в обход межправительственных площадок и механизмов (хотя и с участием представителей государств). Это новое явление в мировой практике, и его дальнейший потенциал и последствия еще предстоит оценить.

Одновременный, но противоположный по смыслу и содержанию процесс связан с нарастающим присутствием и ролью государства в Сети. Одной из его составляющих является стремление государства к укреплению контроля над инфраструктурой Сети в пределах национальной территории. Последовательным сторонником этого подхода является Россия, которая неоднократно озвучивала свои инициативы на международных площадках. Близкие позиции занимают российские партнеры по ШОС. Инициативу создания

в рамках ООН новой международной структуры для координации вопросов управления Интернетом также с 2009 по 2011 г. продвигали страны группы IBSA — Индия, Бразилия и ЮАР, которые также являются партнерами России по БРИКС.

Отправные посылки данного подхода состоят в следующем.

Вопросы управления Интернетом и развития его инфраструктуры должны решаться и обсуждаться в рамках легитимной межправительственной площадки, которая объединяла бы все международное сообщество и желательно действовала под эгидой ООН. Российская Федерация видит такую площадку прежде всего в МСЭ и последовательно продвигает на международном уровне инициативу передачи Союзу электросвязи критических функций Интернета и закрепления в его повестке дня вопросов управления Сетью. Эти тезисы озвучивались российской делегацией в ходе ВКМЭ 2012 г., в рамках всех последних конференций IGF, на NETmundial и т. д. С акцентом на этой инициативе была сформирована российская позиция для Полномочной конференции МСЭ 2014 г.

Для продвижения этой повестки дня также, вероятно, будет задействована площадка итогового саммита ВВУИО+10. На национальном уровне наделение МСЭ ведущей ролью в проработке вопросов управления Интернетом отражено в числе задач «Основ государственной политики России в области МИБ на период до 2020 г.» — доктринального документа, подписанного в 2013 г.

Принцип управления Интернетом с участием всех заинтересованных сторон закреплен в итоговых документах ВВУИО и отражен в повестке дня и формате работы МСЭ, IGF, ряда других структур и, таким образом, не подлежит сомнению. Однако его интерпретация, предлагаемая ICANN и другими структурами технического сообщества и воспроизводимая в рамках таких площадок, как NETmundial, не совсем верна. Необходимость учета мнений заинтересованных сторон помимо государства не дает право принимать решения, которые не учитывают интересы и позиции государства и не согласованы с его представителями. Несмотря на равный статус заинтересованных сторон и необходимость учета всех позиций, именно государства как носители суверенитета и единственные субъекты международного права являются конечной инстанцией принятия решений по вопросам управления Интернетом.

В Интернете в определенной мере действует и применяется принцип государственного суверенитета, пределы которого определяются в том числе национальными границами и юрисдикциями. Отсюда следует правомерность и необходимость проработки вопросов управления Интернетом с учетом существования его национальных сегментов, политики регулирования которых зависят от суверенной воли того или иного государства и потому могут различаться, несмотря на следование общим принципам. При этом не оговаривается отдельно, как рассматривается национальный суверенитет в рамках деятельности международных организаций, в которых состоит Российская Федерация (тот же МСЭ, Совет Европы, ООН и т. п.)

Одним из важнейших элементов нынешнего *status quo*, который подлежит пересмотру в рамках формирования *международной* модели управления критической инфраструктурой Сети, является управление IP-адресацией, доменами, DNS — и, соответственно, роль и статус Корпорации Интернета. В частности, с точки зрения сторонников переноса ключевых функций управления Сетью на площадку МСЭ, ICANN не может считаться оптимальной организационной площадкой для исполнения критических функций Сети и проработки вопросов управления ей в силу следующих причин:

- Корпорация Интернета не является международной организацией и, следовательно, не имеет международно-правовой легитимности для решения глобальных вопросов, затрагивающих все международное сообщество — таких как управление Интернетом.
- Несмотря на формально некоммерческий статус ICANN, программы расширения доменного пространства приносят Корпорации Интернета значительные доходы, что создает конфликт интересов и ставит под сомнение объективность ICANN и учет всего спектра общественных интересов по данным вопросам.
- ICANN не является нейтральной независимой структурой, так как создана и существует в правовом поле США и связана с американским правительством рядом контрактных обязательств и, вследствие этого, может подменять оформление и продвижение согласованной позиции всех заинтересованных сторон поддержкой узкой группы интересов.
- Исполнение ICANN критических функций Сети ущемляет интересы и угрожает безопасности международного сообщества,

так как контроль над исполнением критических функций де-факто имеет правительство США в рамках контрактов с Корпорацией Интернета[1]. Концентрация контроля над Интернетом, который является *международным достоянием*, в руках одного государства называется неприемлемой и на нынешнем этапе уже не оправданной техническими ограничениями.

Вызовы функциональной модели управления Интернетом: политизация и фрагментация

Проблема состоит в том, что параллельное развитие двух описанных выше подходов все чаще ведет к их конкуренции и столкновениям, которые в том числе проявляются на международных площадках.

Ярким примером такого столкновения являются дискуссии и решения в рамках Всемирной конференции по международной электросвязи (ВКМЭ), которая состоялась на площадке МСЭ 3–4 декабря 2012 г. в г. Дубаи, ОАЭ. Ключевой задачей конференции являлось согласование и принятие изменений в Регламент международной электросвязи (РМЭ) — де-факто глобальный договор между членами МСЭ, регулирующий установление общих принципов, касающихся обеспечения и эксплуатации международной электросвязи; обеспечения взаимодействия сетей электросвязи; поддержания гармоничного развития и эффективной эксплуатации технических средств и проч. В последний раз перед ВКМЭ-2012 РМЭ обновлялся в 1988 г., т. е. фактически до распространения в мире Интернета в его современном виде, что и повлекло необходимость его обновления к 2012 г.

В ходе подготовки и проведения ВКМЭ конференции Россия при поддержке Ирана, Китая, ряда государств Африки и арабского мира выдвинула поправки, вводящие в РМЭ вопросы управления Сетью в русле межправительственного регулирования. В частности, исходная версия российских предложений (от 17 ноября 2012 г.):

- вводила в РМЭ понятия и определения Интернета, интернет-трафика, корневой инфраструктуры Интернета, а также национального сегмента Интернета;

[1] Подробно см. раздел VI «Управление глобальной инфраструктурой Сети: в поисках оптимальной модели».

- вводила статью 3.А «Интернет», в рамках которой утверждались равные права государств — членов МСЭ в сфере управления Интернетом, в том числе в части использования и управления ресурсами IP-адресации, распределения и делегирования доменных имен и развития системы DNS, а также суверенное право государств вырабатывать политики управления Интернетом и осуществлять регулирование национальных сегментов Сети и деятельности операторов услуг доступа в национальных границах.

Даже после того как данные предложения были сняты с повестки дня и заменены менее масштабными поправками, консенсуса по тексту Итоговых актов (нового РМЭ) достичь не удалось. Участники вынуждены были отойти от принципа принятия решений консенсусом и устроить голосование, итогом которого стал раскол сообщества стран — членов МСЭ на две крупные поляризованные группы (см. рис. 9).

Хотя итоговый РМЭ в итоге не содержал норм о национальном суверенитете в Интернете (равно как и понятия «интернет»), ход

Рис. 9. Итоги голосования по обновленному РМЭ на ВКМЭ 2012 г. в Дубаи

Источник: IPV Limited

и итоги ВКМЭ в западных странах и структурах технического сообщества были восприняты как атака государств на техническое сообщество, ICANN и сам принцип управления с участием всех заинтересованных сторон. В прессе и широкой общественной дискуссии распространилось мнение о ВКМЭ как начале «холодной войны за Интернет» (что едва ли отражают реальные итоги конференции).

Ожидалось, что попытки закрепить проблематику управления Интернетом с позиций принципов государственного суверенитета в повестке дня МСЭ получат развитие в ходе Полномочной конференции организации, которая прошла с 20 октября по 7 ноября 2014 г. в корейском Пусане. Развитие событий в этом направлении могло бы означать дальнейшее расхождение повестки дня сторонников интернационализации управления Сетью и мультистейкхолдерных организаций технического сообщества.

Другим примером конфликта различных подходов может служить уже упомянутая встреча NETmundial в Сан-Паулу. Несмотря на принятие итогового заявления, представители ряда государств, включая Россию, отказались поддержать этот документ и признавать его отражающим согласованное мнение всех заинтересованных сторон, участвовавших во встрече. В качестве одной из причин был отмечен недостаточно прозрачный процесс работы над текстом итогового заявления, а также недостаточный учет мнений представителей государств и других заинтересованных сторон, в том числе через механизм письменных комментариев.

Несмотря на то что конфликты сторонников различных подходов пока не ведут к инфраструктурным проблемам в Сети и не угрожают ее работе как таковой, их дальнейшее развитие может оказаться разрушительным для экосистемы Глобальной сети из-за ряда негативных последствий.

1. Политизация вопросов, имеющих изначально нейтральный характер, и нерешение практических вызовов и проблем управления Сетью. ВКМЭ 2012 г. в Дубае стала примером того, как технические по своей сути вопросы и инициативы, попав в уже политизированную дискуссию, начинают интерпретироваться неоднозначно. Шквал критики, которую представители технического сообщества и западной интернет-общественности обрушили на новый РМЭ, малопонятен, если рассматривать итоговые акты вне контекста самой конференции и полемики на ее площадке. Политизация

площадки ВКМЭ привела к тому, что статью 7 РМЭ («Незапрашиваемые электронные сообщения») нередко пытались интерпретировать как попытку сторонников «цифрового суверенитета» завуалированно включить в повестку дня МСЭ вопросы регулирования контента в Интернете. Между тем речь идет всего лишь о нейтральной, хотя и не совсем удачной в части формулировок, мере по борьбе со спамом, распространяемым через сети электросвязи, включая Интернет (так и не упомянутый в новом РМЭ). Еще более выраженный и более опасный по своим последствиям пример связан с политизацией вопроса о размещении инфраструктуры корневых серверов DNS и управлении ей (см. раздел VI).

В то же самое время конкретные крупные вопросы в сфере управления Сетью остаются невостребованными и непроработанными в необходимой мере именно в силу смещения внимания и усилий заинтересованных сторон на обсуждение политизированных моментов.

- Спустя два года после разоблачений программ электронного шпионажа АНБ и других спецслужб не выработан никакой международный механизм борьбы с такими явлениями и, более того, не предложена даже стратегия действий глобального интернет-сообщества в этой части. Надежды, которые возлагались на NETmundial в этой части, не оправдались в ходе саммита 2014 г.
- Нарастает потребность в выработке глобальных подходов к вопросам идентификации в Интернете, что остро востребовано как с учетом развития трансграничных сервисов, так и в контексте развития киберпреступности и иных угроз в Сети.
- Не подвержен тщательной многосторонней проработки вопрос сетевой нейтральности (англ. *Net Neutrality*), который прежде всего требует вовлечения в его решение операторов услуг доступа.
- Не менее важны проблемы юрисдикции в Сети, в том числе в отношении трансграничных сервисов; а также вопросы развития облачных сервисов, обработки больших данных (англ. *Big Data*) и проч.

2. Формирование параллельных повесток дня, документов и площадок работы по вопросам управления Интернетом. Развитие трека NETmundial, который не получил поддержки со стороны России

и некоторых других стран, создает прецедент дублирующих друг друга по содержанию повесток дня, которые развиваются в разных направлениях, охватывая все глобальное сообщество заинтересованных сторон.

«Зеркальным» прецедентом являются попытки сформировать повестку дня управления Интернетом на межправительственных площадках без достаточного вовлечения технического сообщества и учета его мнений. Опять же уместен пример ВКМЭ-2012, где из 1576 участников было девять представителей ISOC и 15 представителей региональных интернет-регистратур, которые все равно не могли участвовать в итоговом голосовании.

«Расщепление» глобальной повестки дня в сфере управления Интернетом на уровне различных площадок опасно тем, что создает условия для политической фрагментации. Худший сценарий, который маловероятен в практическом плане, но показывает вектор развития проблемы, — формирование региональных блоков и коалиций государств, корпораций и структур технического сообщества, отстаивающих собственные подходы к вопросам управления Интернетом и игнорирующие инициативы и наработки друг друга.

В сумме обозначенные выше негативные тенденции могут привести к тому, что отдельные участники процесса, не найдя взаимопонимания, решат идти собственными путями уже в плане выработки технических политик и стандартов регулирования Сети. Политическая поляризация и «расщепление» треков управления Интернетом в перспективе могут создать условия для развития автономных политик управления Сетью уже на инфраструктурном уровне.

Наибольшими ресурсами для этого обладают государства — в том числе те, которые являются сторонниками управления Интернетом на международных площадках. Курс на инфраструктурный суверенитет построен на рациональной с точки зрения самих государств мотивации:

- нерешенность проблемы глобального электронного шпионажа и сбора данных пользователей в Интернете. Попытки государств обеспечить безопасность своих систем и граждан самостоятельно ведут их к решениям по локализации данных, созданию собственной канальной инфраструктуры, ужесточению политики в отношении зарубежного ПО и средств защиты информации и проч.;

- контроль над критическими ресурсами и функциями Интернета, как было показано выше, представляет для ряда государств чувствительную тему. Соображения национальной безопасности требуют от них снижения зависимости национальных сегментов сети от глобальной DNS, если другими путями вопрос решить не удается;
- несмотря на крайне спорные экономические эффекты инфраструктурной фрагментации Интернета, развитие инфраструктуры и импортозамещение в национальных сегментах привлекательно для ряда игроков интернет-сектора.

В практическом смысле процессы автономизации сегментов Интернета могут проявляться почти на всех уровнях его инфраструктуры (см. табл. 5).

Таблица 5. Некоторые возможные направления автономизации сегментов Интернета по уровням базовой эталонной модели взаимодействия открытых систем (модель ISO/OSI)

№	Уровень	Умеренный вариант (автономизация сегментов Сети)	Жесткий/крайний вариант (фрагментация Сети)
1–2	Физический и канальный уровни (*Physical layer and data link layer*)	1. Разработка и внедрение государствами либо иным сообществами стандартов протоколов физического уровня в обход IETF. 2. Локализация в национальных границах DNS-серверов верхнего уровня, обслуживающих TLDs (в том числе страновые)	1. Перестройка магистральной канальной инфраструктуры (оптоволоконные каналы и проч.) на национальном/региональном уровнях с целью максимального сокращения количества каналов физической трансграничной передачи данных. 2. Создание в национальном/региональном масштабе системы квазисистемы IP-адресации с целью обеспечения относительной автономии от глобальной DNS. 3. Создание новой системы корневых серверов и аналога существующей системы DNS для обеспечения полной автономии собственного сегмента Сети

Окончание таблицы 5

№	Уровень	Умеренный вариант (автономизация сегментов Сети)	Жесткий/крайний вариант (фрагментация Сети)
3	Сетевой/ межсетевой уровень (*Network layer*)	Замедление/прекращение сотрудничества заинтересованных сторон, взявших курс на автономизацию интернет-сектора, с техническим сообществом по вопросам внедрения IPv6 и совершенствования протоколов сетевого уровня	Запретительное импортозамещение программно-аппаратных средств, обеспечивающих передачу данных на сетевом уровне (маршрутизаторы и проч.) из соображений информационной безопасности
4–5	Транспортный уровень (*Transport layer*) и сеансовый уровень (*Session layer*)		Разработка и внедрение государствами либо иными сообществами стандартов протоколов транспортного и сеансового уровней в обход IETF и других структур технического сообщества
6	Уровень представления (*Presentation layer*)	Запретительное регулирование сервисов и программно-аппаратных средств, использующих иностранные стандарты шифрования данных на уровне представления (применительно к России — RSA, SSL и проч.)	
7	Уровень приложений (*Application layer*)	1. Прекращение сотрудничества отдельных государств / групп государств с ICANN и региональными регистратурами по вопросам внедрения программы DNSSEC. 2. Широкий ввод в эксплуатацию программно-аппаратных средств фильтрации и перенаправления DNS-запросов на национальном/региональном уровнях с целью регулирования трансграничного доступа к контенту в Интернете	1. Запрет/ограничение трансграничной передачи данных в Сети по незащищенным протоколам уровня приложений (HTTP) на уровне отдельных государств / групп государств. 2. Перенос на национальную территорию серверов и центров обработки персональных данных граждан того или иного государства вне зависимости от юрисдикции сервисов, осуществляющих обработку

Несмотря на то что сегодня Интернет сохраняет свое инфраструктурное и архитектурное единство, нарастание политизации вопросов управления им может привести к реальному движению в сторону автономизации его сегментов. Некоторые из перечисленных в таблице 5 мер и решений уже получили практическое развитие.

- В 2013 г. разоблачения Эдварда Сноудена подтолкнули Бразилию и ФРГ к проработке возможностей переноса на национальную территорию дата-центров, обрабатывающих персональные данные их граждан. Германия, кроме того, приступила к изучению возможностей создания национальной закрытой сети для государственных органов. В России шаг в сторону локализации обработки и хранения персональных данных российских граждан был сделан в 2014 г. с принятием Федерального закона от 21.07.2014 № 242-ФЗ. Сформулированные в нем поправки в текст 152-ФЗ «О персональных данных» вступили в силу 1 сентября 2015 г.
- За последние годы китайские специалисты направили в IETF несколько редакций мемо с описанием технологии квазиадресации, дублирующей функции национального сегмента DNS.
- В апреле 2014 г. стало известно о предложениях по перестройке архитектуры Сети в российском сегменте, который подготовила рабочая группа при администрации президента России. В частности, предлагалось перенести на российскую территорию DNS-сервера верхнего уровня, которые обслуживают запросы по доменным зонам .ru и .рф, а также ввести трехуровневую иерархию интернет-провайдеров в России (местный–региональный–федеральный уровни) и ограничить возможность трансграничной передачи трафика через сети провайдеров местного и регионального уровня. Предложения были раскритикованы российской интернет-отраслью и по состоянию на ноябрь 2015 г. не получили развития.
- В октябре 2014 г. СМИ сообщали о планировании закрытого заседания Совета Безопасности РФ после проведенных Минсвязи РФ летом 2014 г. киберучений с участием ФСБ РФ, ФСО РФ, Минобороны РФ, МВД РФ, точки обмена трафиком MSK-IX, а также Координационного центра доменов .ru/.рф. В ходе учений, по имеющейся открытой информации, среди прочих моделей угроз отрабатывался сценарий нарушения функционирования российского сегмента Интернета в результате

«внешних недружественных воздействий». По итогам учений помощник президента РФ И.О. Щеголев в интервью СМИ заявил, что состоявшиеся учения продемонстрировали «недостаточную устойчивость Рунета», а также отметил, что рычаги управления глобальной инфраструктурой сетью, включая DNS и систему распределения ресурсов нумерации, до сих пор находятся в руках США. В апреле 2015 г. сообщалось о том, что главой Минкомсвязи РФ Н.А. Никифоровым подготовлен доклад для правительства России, посвященный вопросам обеспечения безопасности и устойчивости российского сегмента Интернета и отражающий итоги киберучений лета 2014 г. По информации СМИ, в докладе упоминается необходимость резервирования системы корневых DNS-серверов, а также дублирующего реестра IP-адресов. В апреле 2015 г. российский представитель, выступая на одном из международных мероприятий в формате *Трек полтора*, отметил, что вынужденной реакцией России и ее союзников на проведение политики США и стран Запада по осуществлению глобального электронного шпионажа и активному наращиванию потенциала использования ИКТ в военно-политических целях может в конечном счете стать создание безопасной информационной инфраструктуры, альтернативной нынешнему Интернету.

Глобальная система DNS, которая в отличие от большинства уровней инфраструктуры осуществляет свои функции централизованно и не может быть реформирована в сжатые сроки, является одним из принципиальных звеньев в контексте автономизации сегментов Сети. На сегодня в рамках ГПЭ ООН было достигнуто понимание того, что ряд принципов международного права, включая принцип государственного суверенитета, применяются к ИКТ-инфраструктуре. В том числе такой принцип распространяется и на инфраструктуру DNS, а государства имеют право обеспечивать безопасность и стабильность национальных сегментов DNS в соответствии со своими собственными интересами и политикой. Одним из таких способов является создание дублирующей инфраструктуры для обеспечения автономной работы национальных сегментов DNS в кризисной ситуации.

Однако чрезмерное движение в этом направлении может представлять угрозу для всей экосистемы Интернета, ключевым свой-

ством которой является ее единство. Наибольшей опасностью в случае реализации жестких сценариев представляется фрагментация Сети по национальным или региональным сегментам. Ценой неспособности заинтересованных сторон и государств найти оптимальный баланс полномочий и модель управления критическими ресурсами может стать торможение развития Интернета как ключевой производительной, научной, торгово-финансовой, культурной и инновационной силы последних двух десятилетий.

Угроза

Замедление развития глобального интернет-сектора вследствие политически обусловленной фрагментации Интернета по национальным и региональным сегментам в горизонте 2018–2020 гг.

Деполитизация управления Сетью и дальнейшие шаги в рамках подготовки к ВВУИО+10

Одним из ответов на обозначенные выше вызовы может стать возвращение всех участников процесса управления Интернетом и сторонников разных подходов к некой «точке согласия», частичный «перезапуск» дискуссии по ключевым вопросам управления Сетью между представителями разных подходов. К преодолению противоречий — или продуктивному взаимодействию, невзирая на их наличие, — стороны может подтолкнуть совместная работа над глобальным документом, который по своим задачам, формату и процессу выработки отвечал бы интересам как технического сообщества, так и сторонников международного регулирования Сети.

Ключевое условие самой возможности начала работы над таким документом — это выбор компромиссной площадки, которая является:

- глобальной, актуальной для всех членов мирового сообщества;
- обеспечивающей участие всех заинтересованных сторон;
- имеющей нейтральный статус и не ассоциируемой с каким-либо отдельным государством либо организацией интернет-сообщества или какой-либо группой интересов межправительственного либо иного характера.

Из существующих форматов этим критериям отвечает Форум по вопросам управления Интернетом. «Слабость» форума

в процедурном и исполнительном смысле может оказаться его преимуществом с точки зрения нейтрального, неангажированного статуса, она делает его площадку политически приемлемой для всех заинтересованных сторон, включая правительства.

В этой связи своевременным шагом видится выдвижение инициативы по переформатированию IGF в постоянную рабочую площадку по подготовке глобального соглашения в сфере управления Интернетом в горизонте двух-трех лет (до 2018 г.). Цель документа может состоять в согласовании и кодификации в рамках международно-правовых механизмов ключевых принципов управления Интернетом. Оптимальным форматом для осуществления такой работы могли бы стать конвенция или договор ООН, которые вобрали бы в себя основные фактически разделяемые принципы управления Интернетом: участие всех заинтересованных сторон, открытость, сетевую нейтральность, целостность и связность Сети и проч. Кроме того, в документе могли бы, наконец, получить достойное отражение вопросы пресечения эксплуатации Интернета государством в неправомерных целях и защиты права на тайну частной жизни в Сети.

Одним из ориентиров в смысле концепции документа мог бы выступать принятый резолюцией 2222 (XXI) Генеральной Ассамблеи ООН от 19.12.1966 «Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела» («Договор о Луне»), не прописывающий конкретные обязательства сторон, но фиксирующий общие принципы сотрудничества. Несмотря на то что договор дефакто не достиг целей, для которых был создан и открыт к подписанию (ведущие космические державы до сих пор не присоединились к нему), он предлагает любопытную модель сотрудничества государств в пространстве, которое, как и Интернет, не подлежит однозначному делению на национальные сегменты и юрисдикции.

Движение в этом направлении потребует:

- расширения и продления мандата форума, стабилизации механизма его финансирования при расширении его объемов;
- переформатирования IGF в постоянную рабочую площадку по подготовке международного договора — в частности, за счет преобразования его секретариата в постоянно действующий рабочий аппарат, который будет действовать в круглогодичном режиме (исполнительный секретариат);

- согласования в рамках саммита ВВУИО+10 в 2016 г. и включения в его итоговые документы плана действий по изменению структуры и задач IGF.

  Согласование этих положений может быть достигнуто при условии консолидации усилий заинтересованных сторон и участия государств в поддержке этой инициативы; в частности, с единой позицией по этому вопросу в рамках ВВУИО могла бы выступить Россия со своими партнерами по БРИКС;
- формирования при исполнительном секретариате рабочих и экспертных групп, на постоянной основе прорабатывающих ключевые вопросы и принципы, которые могли бы найти отражение в итоговом международном документе (сетевая нейтральность, защита права на тайну частной жизни и установление предпосылок для ее систематических нарушений АНБ США и спецслужбами других государств в последние годы; локализация данных и преодоление угрозы фрагментации Сети на инфраструктурном уровне и т. д.).

При конструктивном подходе к этим задачам со стороны государства и других заинтересованных сторон возможно было бы надеяться на начало работы над глобальным документом в 2016 г. и завершение его подготовки до конца 2017–2018 гг.

В целях более полного и эффективного учета интересов государств в рамках процесса управления Интернетом с участием всех заинтересованных сторон необходимо усиление механизмов их вовлечения в принятие решений на существующих в этой сфере площадках.

В этой связи могут быть востребованы предложения по усилению механизма Консультативного правительственного комитета (GAC) ICANN в общей структуре принятия решений в рамках Корпорации Интернета.

На протяжении процесса передачи функций IANA, который может оказаться довольно длительным, закрепление за представителями государства права «особого голоса» могло бы способствовать нужной коррекции и оптимизации направления этого процесса с учетом интересов государств как одной из важнейших заинтересованных сторон.

В этой связи целесообразно поддержать идею поправок в Устав ICANN, впервые опубликованную 15 августа 2014 г. и обсуждающуюся

сообществом до сих пор. Суть предложения — повысить барьер голосования, который требуется преодолеть Правлению ICANN для того, чтобы не утвердить то или иное решение Консультационного правительственного комитета (GAC). Барьер предлагается поднять с простого большинства голосов правления до не менее чем двух третей.

Процесс ВВУИО+10, очередной этап которого в формате министерской встречи пришелся на декабрь 2015 г., в 2016 г. и далее может быть использован для продвижения принципа деполитизации вопросов глобального управления Интернетом. В частности, могут быть сформированы предложения по отделению друг от друга:

- вопросов выработки политик в сфере управления Сетью (подготовка международного договора о принципах управления Интернетом, развитие глобального доменного пространства, выработка подходов по защите права на тайну частной жизни в Сети);
- решения технических задач (присвоение и распределение параметров протоколов в Сети, развитие сервиса идентификации владельцев доменных имен WHOIS, продолжение и активизация внедрения IPv6 и DNSSEC, усиление шифрования пользовательского трафика с целью защиты персональных данных);
- администрирования системы управления Интернетом (структура управления корневыми серверами DNS, механизмы выработки решений в рамках рабочей группы по проектированию Интернета (запросы комментариев — RFC) и других организаций технического сообщества).

Не вызывает сомнений, что многие вопросы, такие как передача контроля над исполнением функций IANA, носят комплексный характер и не могут не рассматриваться в том числе в политическом контексте. Но даже частичное разведение повестки дня там, где это возможно, могло бы способствовать ее более предметному и неангажированному наполнению, а также снижению риска конфронтации между различными заинтересованными сторонами.

Одной из задач на ближайшую перспективу в этой связи видится внесение данных предложений в повестку дня процесса ВВУИО+10 на стадии министерской встречи в декабре 2015 г., а также на возможной последующей стадии глобального саммита в 2016 г.

Помимо разрешения политических противоречий, связанных с архитектурой глобального управления Сетью, требуется активизация усилий по внедрению на национальном и глобальном уровне ряда технических решений, обеспечивающих безопасность в Интернете и стабильность работы Глобальной сети.

Развитие инфраструктуры уникальных идентификаторов Интернета: поддержка внедрения IPv6 и DNSSEC

Одной из важных и актуальных задач для международного сообщества и, в частности, России, остается полномасштабное внедрение обновленной версии IP-протокола — IPv6 и обеспечение его совместимости с прежней версией — IPv4. Проблема внедрения IPv6 возникла уже достаточно давно — последний диапазон свободных адресов IPv4 был распределен в еще феврале 2011 г.

Однако темпы ее решения, связанного с внедрением стандарта IPv6 параллельно с продолжением функционирования прежней версии — IPv4, являются недостаточными. По данным Cisco Systems, по состоянию на июнь 2014 г., спустя два года после

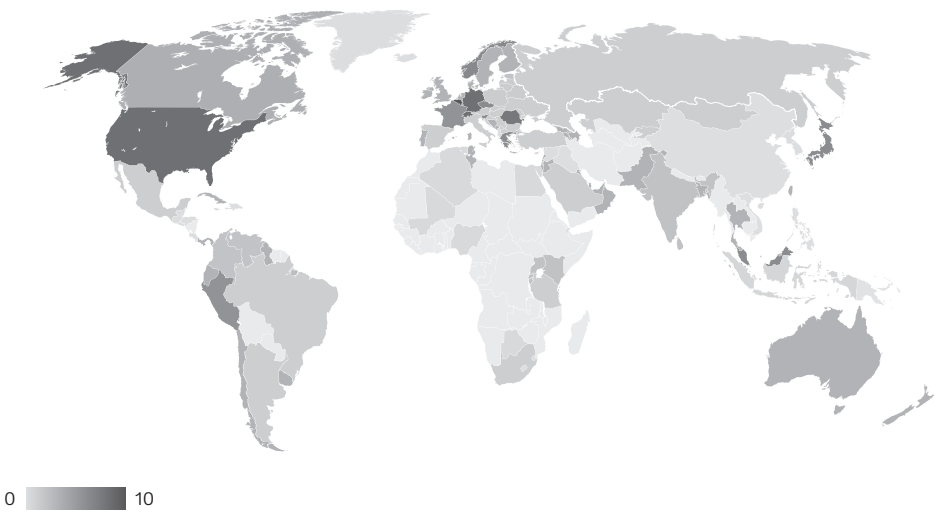


Рис. 10. Уровень внедрения IPv6 в % по странам мира по состоянию на июнь 2014 г.

Примечание: внедрение IPv6 в России — 12,92% в общей сложности».

Источник: Cisco Systems

запуска процесса внедрения IPv6 в глобальном масштабе, обновленный протокол обеспечивал доступ в Сеть на всех этапах лишь 4% пользователей, даже в США их доля составляла 8%. Развитие магистральной технологической тенденции на оснащение доступом в Сеть большинства бытовых, промышленных и иных объектов — Интернета вещей требует значительного ускорения темпов внедрения IPv6 в мире. По прогнозам, к 2020 г. к Сети будут подключены до 50 млрд устройств, что более чем десятикратно превышает весь диапазон адресов IPv4; еще через десять лет речь может идти о триллионах устройств. Причем потенциальные экономические эффекты Интернета вещей (вклад в глобальный ВВП на уровне 10–15 трлн долл. США в течение ближайших 20 лет, по оценкам General Electrics) делает создание максимально благоприятных условий для его развития безусловным приоритетом для государств и технического сообщества.

В этой связи своевременным видится оказание государством активного содействия по внедрению IPv6 на национальном уровне.

Примером активной работы государства во взаимодействии с техническим сообществом и другими заинтересованными сторонами является правительство КНР, которое приняло комплексный национальный десятилетний план внедрения IPv6 в апреле 2012 г. Разработка, принятие и активная реализация аналогичного национального плана внедрения IPv6, например, на 2015–2020 гг. представляются актуальной задачей для России и отечественного интернет-сообщества. Процесс разработки и принятия такого документа мог бы осуществляться профильными государственными органами в тесном взаимодействии со всеми заинтересованными сторонами, включая региональные регистратуры (RIRs), регистраторов и иных представителей интернет-сектора и технического сообщества.

Аналогичных мер и усилий может потребовать внедрение DNSSEC (англ. *Domain Name System Security Extensions*) — набора расширений протокола DNS, позволяющих нейтрализовать атаки, связанные с подменой DNS-адреса, за счет использования цифровых подписей. Несмотря на успехи, достигнутые с момента выпуска первой спецификации DNSSEC (RFC 2065 в 1997 г.), — подписание корневой зоны DNS к июлю 2010 г., подписание зоны .com в марте 2011 г., подписание зон .ru и .рф в ноябре–декабре 2012 г., общий уровень внедрения DNSSEC в России и мире пока не пре-

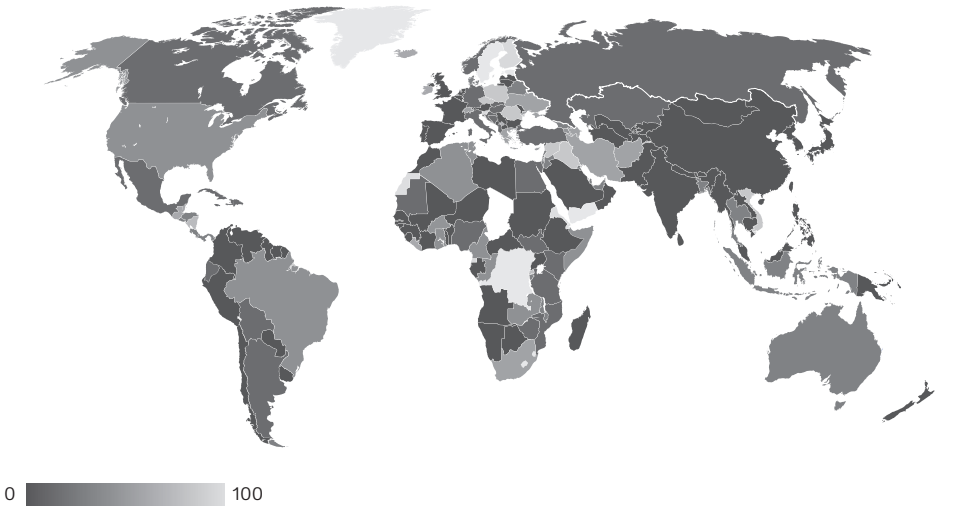


Рис. 11. Уровень внедрения протокола DNSSEC по странам мира в % по состоянию на 2014 г.

Источник: The Internet Society

вышает 10–15%, что обусловливает высокую уязвимость перед атаками типа подмены DNS-адреса.

Отраслевые ведомства (Минсвязи РФ) при содействии технических организаций (региональных регистратур Интернета, IETF), местных интернет-регистратур (LIRs) и провайдеров доступа в Интернет могли бы сформировать программы содействия внедрению DNSSEC на национальном уровне.

Дополнительная информация

1. Якушев М. Интернет-2012 и международная политика // Индекс безопасности. 2013. № 1 (104). С. 29–42.
2. Касенова М. Глобальное управление Интернетом в контексте современного международного права // Индекс безопасности. 2013. № 1 (104). С. 43–64.
3. The Internet of Things: Making sense of the next mega-trend. IoT primer. 01.09.2014. URL: http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf (дата обращения: 01.03.2016).
5. The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. White Paper. Dave Evans, Cisco Systems. April

2011. URL: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (дата обращения: 01.03.2016).
6. Курбалийя Й. Управление Интернетом. М.: Координационный центр доменов .ru/.рф, 2010.

Документы

1. Заключительные акты Всемирной конференции по международной электросвязи (Дубай, 2012 г.). Международный союз электросвязи, 2012. URL: http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12-ru.pdf (дата обращения: 01.03.2016).
2. Основные элементы официальной позиции Российской Федерации по итогам Глобальной встречи по вопросам управления Интернетом. Посольство Российской Федерации в Аргентинской Республике. 19.06.2014. URL: http://argentina.mid.ru/-/19-06-2014-osnovnye-elementy-oficial-noj-pozicii-rossijskoj-federacii-po-itogam-global-noj-vstreci-po-voprosam-upravlenia-internetom (дата обращения: 01.03.2016).
3. Комиссия по стратегии: роль ICANN в экосистеме управления Интернетом (окончательная версия). 2014.23.05. Веб-сайт ICANN. URL: https://www.icann.org/ru/system/files/files/ig-ecosystem-report-23may14-ru.pdf (дата обращения: 01.03.2016).
4. NETmundial Multistakeholder Statement. Global Multistakeholder Meeting on the Future of Internet Governance. April 24, 2014. URL: http://netmundial.br/ru/netmundial-multistakeholder-statement/ (дата обращения: 01.03.2016).

Раздел VI

Управление глобальной инфраструктурой Сети: в поисках оптимальной модели

Координация работы критической инфраструктуры Интернета сегодня вписана в уникальную организационную и архитектурную модель, не имеющую прямых аналогов в международной практике. Центральное место в этой модели занимает вышеупомянутая Корпорация Интернета по присвоению имен и номеров (ICANN), которая отвечает за обеспечение работы двух ключевых уровней инфраструктуры Интернета — IP-адресов и доменных имен, так называемых уникальных идентификаторов Интернета.

Еще до того, как в 1998 г. была создана сама ICANN, американские власти по мере развития Интернета и его коммерциализации решили начать процесс передачи критической инфраструктуры Сети в руки сообщества технических специалистов. В июне 1997 г. Национальное управление по телекоммуникациям и информации (NTIA) — агентство Министерства торговли США — опубликовало Запрос комментариев (RFC) относительно «текущей и будущей системы регистрации доменных имен Интернета». В январе 1998 г. NTIA опубликовало «Зеленую книгу», — доклад, предлагавший для комментариев предварительное видение пути приватизации управления системой DNS и постепенному отказу правительства США от этой функции.

Итогом этого процесса стало опубликованное NTIA 5 июня 1998 г. с учетом рассмотренных комментариев заявление о политическом курсе — «Белая книга». В документе интернет-сообществу предлагалось создать частную некоммерческую корпорацию для управления DNS и осуществление функций администрации адресного пространства Интернет (функции IANA). В развитие положений «Белой книги» 25 ноября 1998 г. Министерство торговли США подписало Меморандум о взаимопонимании (MoU) с ICANN, в котором Корпорация Интернета официально признавалась частной некоммерческой организацией, которая фигурировала в «Белой книге». Чуть позднее, в феврале 2000 г. эти же стороны заключили на безальтернативной основе еще один контракт — договор

на выполнение корпорацией ICANN технических функций IANA, который далее неоднократно продлевался.

На момент начала активной фазы процесса передачи ответственного управления функциями отношения Корпорации Интернета с правительством США по поводу этих функций регулировались некоммерческим контрактом на 0 долл. от 10 января 2012 г. Срок действия контракта должен был истечь 30 сентября 2015 г. Однако за Министерством торговли США были закреплены два опциона на его одностороннее продление — до сентября 2017 г. и до сентября 2019 г. соответственно. Когда по итогам 53-й конференции ICANN в Буэнос-Айресе стало понятно, что завершить передачу управления функциями IANA не удастся до истечения контракта, правительство США использовало первый опцион. Однако контракт был продлен лишь на год — до конца сентября 2016 г. Причина неполного использования опциона проста — растягивание процесса еще на два года во многом стало бы в глазах как его участников, так и всего технического сообщества (и представителей правительств в частности) констатацией его провала.

Основные функции администрации адресного пространства Интернета

Основные функции IANA:

1. Координация присвоения технических параметров протоколов, по которым работает Интернет.
2. Администрирование файла корневой зоны системы DNS и некоторые другие функции, связанные с работой системы корневых серверов DNS.
3. Распределение адресных ресурсов Интернета — доменных имен верхнего уровня (TLDs) и блоков IP-адресов.
4. Управление доменом верхнего уровня .int и доменом .arpa, зарезервированным для специальных технических целей, связанных с обеспечением работы системы DNS.

Критический характер. Неисполнение либо ненадлежащее исполнение любой из этих функций (с определенными оговорками в отношении четвертой) повлечет нарушение нормальной работы Интернета в глобальном масштабе.

Исполнение и контроль. Функции IANA исполняются командой технических специалистов в рамках обособленного департамента Корпорации Интернета. Формальный контроль исполнения осуществляется правительством США в лице Национальной администрации по телекоммуникациям и информации (NTIA) на основании контракта на осуществление функций администрации адресного пространства Интернет

(IANA) от 10 января 2012 г. Срок действия некоммерческого контракта истек 30 сентября 2015 г., однако Министерство торговли приняло решение об использовании опциона на его продление. Новая и, как считается, окончательная дата прекращения действия контракта — 30 сентября 2016 г.

Полномочия Правительства США:

1. Национальная администрация по телекоммуникациям и информации утверждает запросы ICANN на внесение изменений в файл корневой зоны DNS.
2. Корпорация Интернета предоставляет Министерству торговли США регулярную отчетность об осуществлении данных функций.
3. Правительство США располагает полномочиями для проведения инспекций и проверки исполнения функций IANA.

Ряд государств, включая Россию, последовательно подвергали критике эту институциональную конструкцию. В качестве основного повода для критики указывается тот факт, что два критических уровня инфраструктуры Глобальной сети, управление которыми осуществляется централизованно, находятся в компетенции американской корпорации, существующей в правовом поле штата Калифорния и подконтрольной американскому же правительству. В этой связи различными государствами делались заявления об избыточной и неоправданной концентрации контроля над управлением критическими ресурсами Сети в руках США и недостаточного участия других стран. С 1998 г. Россия устами МИД призывала к пересмотру существующей модели и незамедлительной передачи отдельных либо всех функций IANA международному сообществу, понимая под таковым межправительственную площадку ООН, и в частности МСЭ. За последние годы вопрос неоднократно выносился на повестку дня на глобальных площадках, включая дубайскую ВКМЭ 2012 г., однако не был решен.

Новый виток изменения политики ICANN и ее взаимоотношений с правительством США запустили во многом события лета 2013 г., подорвавшие авторитет Белого дома в вопросах соблюдения прав и свобод человека в Сети — а также частично в сфере управления Интернетом. В разгар событий, связаных с разоблачениями Сноудена, в октябре 2013 г. президент ICANN Фади Шехаде на площадке IGF 2013 объявил о намерении вывести Корпорацию Интернета из-под контроля правительства США. Спустя полгода последовал ответ со стороны Министерства торговли США — 14 марта 2014 г. на сайте NTIA появилась публикация, в которой

излагалось намерение ведомства «передать ключевые функции системы доменных имен DNS глобальному сообществу заинтересованных сторон». Именно это решение определяет контекст проблемы передачи контроля над исполнением критических функций Сети (функций IANA) на сегодняшний день.

Объявленное намерение о передаче функций IANA ставит перед международным сообществом и заинтересованными сторонами следующие вопросы и вызовы.

Открытый вопрос эффективности новой институциональной модели ответственного управления функциями IANA и доверия к ней глобального сообщества заинтересованных сторон. Структура, представленная в итоговом Предложении ICG от 10 марта 2016 г., отвечает требованиям NTIA. Однако ее эффективность, полнота регионального представительства и равные возможности участия заинтересованных сторон пока не проверены на практике. В случае принятия эта схема первое время будет оставаться уравнением со многими неизвестными, и формирование доверия к ней как технического сообщества, так и зарубежных правительств потребует времени и усилий. Организационная схема еще может подвергнуться неоднократной доработке. Таким образом, даже с учетом итогового Предложения ICG передача ответственного управления функциями IANA Transition представляет собой уходящий в будущее процесс с открытым исходом.

Политизация процесса передачи контроля над функциями IANA, равно как и избыточная политизация вопросов, связанных с управлением критическими ресурсами Сети в целом. Характерным примером является политизация дискуссии об управлении корневыми серверами DNS, которую в том числе ведет Россия на международных площадках. Критику вызывает преимущественная концентрация корневых серверов на территории США (10 из 13) и тот факт, что политики управления ими вырабатываются в рамках Консультативного комитета по системе корневых серверов на площадке ICANN. Однако технологические процессы развития корневой инфраструктуры Интернета за последние полтора десятилетия привели к существенному изменению ситуации. На сегодняшний день функции каждого из исходных 13 корневых серверов дублируются его многочисленными «зеркалами», которые достаточно равномерно рассредоточены по различным странам и регионам. Так, на территории России сегодня размещаются три «зеркала»

корневого сервера L, а также по одному «зеркалу» серверов F, J и K. А общее число физических площадок размещения корневых серверов вместе с их «зеркалами» в мире достигло 493 (см. рис. 12).

Также орган, осуществляющий координацию управления корневыми серверами DNS, — Консультативный комитет системы корневых серверов DNS (ККСКС) — изначально сформирован правлением ICANN, однако не подчиняется ему в своей работе и решениях. Входящие в него компании и структуры, которые осуществляют управление тем или иным корневым сервером, также являются самостоятельными субъектами и не связаны обязательствами перед ICANN в части своей оперативной работы. Таким образом, на данный момент вопросы размещения корневых серверов DNS и управления ими не выглядят приоритетными с точки зрения интересов как глобального интернет-сообщества, так и России.

Нерешенность вопросов, связанных с частичным сохранением контроля правительства США над исполнением отдельных критических функций Интернета даже в случае передачи контроля над функциями IANA. Частным случаем являются функции американского интернет-гиганта VeriSign, в которые, согласно его собственному контракту с NTIA, входит техническое редактирование файла корневой зоны DNS (своеобразного каталога IP-адресов и доменных

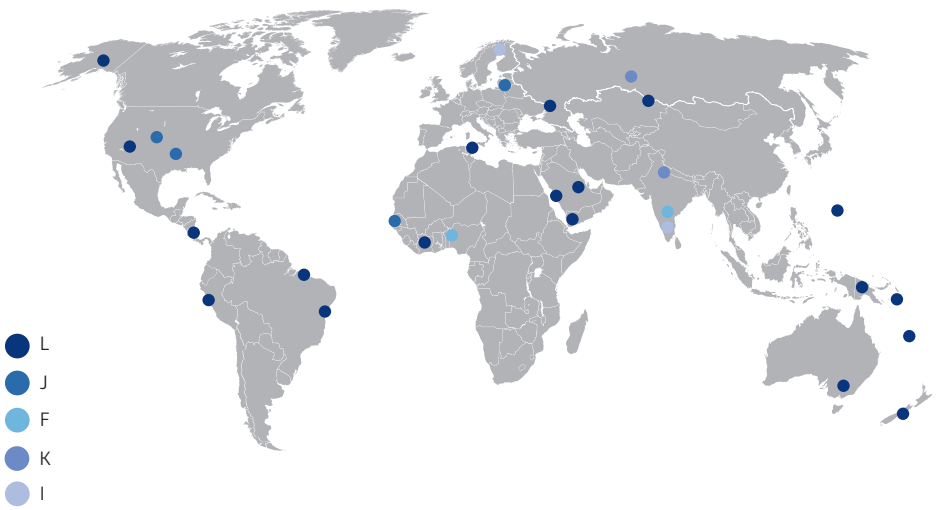


Рис. 12. Расположение корневых серверов DNS по состоянию на июнь 2014 г.

Источник: root-servers.org

имен верхнего уровня), его публикация и рассылка операторам корневых серверов DNS. Передача контроля над функциями IANA от правительства США формально никак не влияет на обязательства VeriSign, хотя в ходе мероприятий ICANN отмечалось, что эти вопросы должны рассматриваться в одной связке.

Исходя из описанной ситуации, возможно сформулировать некоторые общие рекомендации заинтересованным сторонам в России и за рубежом:

- Более активное и системное участие российского интернет-сообщества и правительства в новой экосистеме организаций и рабочих процессов по исполнению функций управления уникальными идентификаторами Интернета. Реалистично исходить из того, что передача ответственного управления функциями IANA формально осуществится до конца 2016 г. Но весь процесс трансформации Корпорации Интернета и отхода правительства США от надзора над критическими функциями Интернета на этом не закончится. Становление новой экосистемы растянется на годы, в том числе в плане настройки механизмов разрешения споров и конфликтов, отладки системы оценки качества работы новой IANA и получения обратной связи от сообщества.
- Уход от представления об ICANN и IANA как о монопольных, исключительных субъектах управления системой уникальных идентификаторов Интернета. Вместо единой площадки ICANN, которая многими воспринималась в качестве «центрального регулятора», возникает возможность «мягкого дрейфа» друг от друга структур технического сообщества, ответственных за разные функции. Прежде всего, речь идет о РРИ и конкретно RIPE NCC. Не менее важно участие в рабочей деятельности IETF и Совета по архитектуре Интернет, составлении RFC, инициативах сообщества сетевых операторов.
- Международное закрепление принципа ответственного и независимого контроля над исполнением критических функций Интернета с участием всех заинтересованных сторон, включая правительства. Речь может идти о международной декларации или договоре, который бы закреплял приверженность государств и глобального сообщества тем принципам, на которых сегодня должно и впредь опираться управление глобальной инфрастрактурой Интернетом, независимо от дальнейшего развития процесса IANA Transition. Такой процесс может получить

развитие в рамках площадки Форума по управлению Интернетом (IGF) и послужить легитимации процесса IANA Transition.

Цель к 2017 г.

Завершение передачи контроля над критическими функциями Интернета (функции IANA) от правительства США независимой международной структуре, сформированной с участием всех заинтересованных сторон и обладающей независимостью от Корпорации Интернета в части согласования и принятия решений.

Дополнительная информация

1. Демидов О. Послесловие из Сингапура: кому США сдают ключи от Интернета? Блог ПИР-Центра, 28.03.2014. URL: http://www.ircenter.org/blog/view/id/162 (дата обращения: 01.03.2016).
2. Касенова М.Б. Глобальное управление Интернетом в контексте современного международного права // Индекс безопасности. Весна 2013. № 1 (104). С. 43–64.

Документы

1. IANA Functions Contract. 2012 Contract. Веб-сайт Национальной администрации США по телекоммуникациям и информации. URL: http://www.ntia.doc.gov/page/iana-functions-purchase-order (дата обращения: 01.03.2016).
2. Предложение о передаче координирующей роли в исполнении функций Администрации адресного пространства Интернета (IANA) Национальным управлением по телекоммуникациям и информации (NTIA) Министерства торговли США глобальному сообществу заинтересованных сторон. Март 2016 года. URL: https://www.icann.org/ru/system/files/files/iana-stewardship-transition-proposal-10mar16-ru.pdf (дата обращения: 01.03.2016).
3. ICANN's Major Agreements and Related Reports. Веб-сайт ICANN URL: https://www.icann.org/resources/pages/agreements-2012-02-25-en (дата обращения: 01.03.2016).
4. NTIA Announces Intent to Transition Key Internet Domain Name Functions. National Telecommunications and Information Administration (NTIA). United States Department of Commerce. March 14, 2014. URL: http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (дата обращения: 01.03.2016).

Раздел VII

Генеральная Ассамблея Организации Объединенных Наций призывает все государства:

a) уважать и защищать право на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации;

b) принимать меры с тем, чтобы положить конец нарушениям этих прав и создавать условия для предотвращения таких нарушений, в том числе путем обеспечения того, чтобы касающееся этого национальное законодательство соответствовало их международным обязательствам по международному праву прав человека;

c) провести обзор своих процедур, практики и законодательства, касающихся слежения за сообщениями, их перехвата и сбора личных данных, включая массовое слежение, перехват и сбор, в целях защиты права на неприкосновенность личной жизни путем обеспечения полного и эффективного выполнения всех их обязательств по международному праву прав человека.

Резолюция Генеральной Ассамблеей ООН
от 18.12.2013 A/RES/68/167
«Право на неприкосновенность личной жизни в цифровой век»

Левиафан в Сети: защита права на тайну частной жизни после событий 2013 г.

За небольшой промежуток времени начиная с июня 2013 г. бывший сотрудник Агентства национальной безопасности (АНБ) США Эдвард Сноуден оказал огромное влияние на международную политику, общественную и экспертную дискуссию в сфере ИКТ, управления Интернетом и, прежде всего, соблюдения прав пользователей на тайну частной жизни в Сети. Несмотря на то что сообщество технических экспертов в сфере информационной безопасности имело представление о ключевых практиках, раскрытых Сноуденом широкой общественности, эффект совершенных разоблачений представляется отчетливым и необратимым.

Информация, раскрытая экс-сотрудником Агентства национальной безопасности (АНБ) США Эдвардом Сноуденом, продемонстрировала политическим лидерам и международной общественности глубину кризиса доверия в отношениях государства со своими партнерами в мире, а также со своими собственными гражданами и гражданами других стран.

Международно-политический итог разоблачений Сноудена несводим к удару по авторитету США в вопросах защиты прав и свобод человека в Сети.

Он фундаментальнее и заключается в констатации того, что ИКТ и Интернет являются не только глобальным генератором прогресса, но и инструментом систематического одностороннего контроля государства над обществом и внешними контрагентами. Не неся ничего фундаментально нового для технических специалистов, разоблачения программ АНБ подтвердили, что кибершпионаж, киберагрессия и незаконный сбор персональных данных в Сети в должном масштабе несут стратегическое преимущество для государств, которые практикуют такие методы, и в то же время создают стратегическую угрозу безопасности и интересам стран — объектов такой деятельности.

ИКТ и Интернет обусловили для шпионажа и вторжения в частную жизнь возможности, никогда не существовавшие прежде:

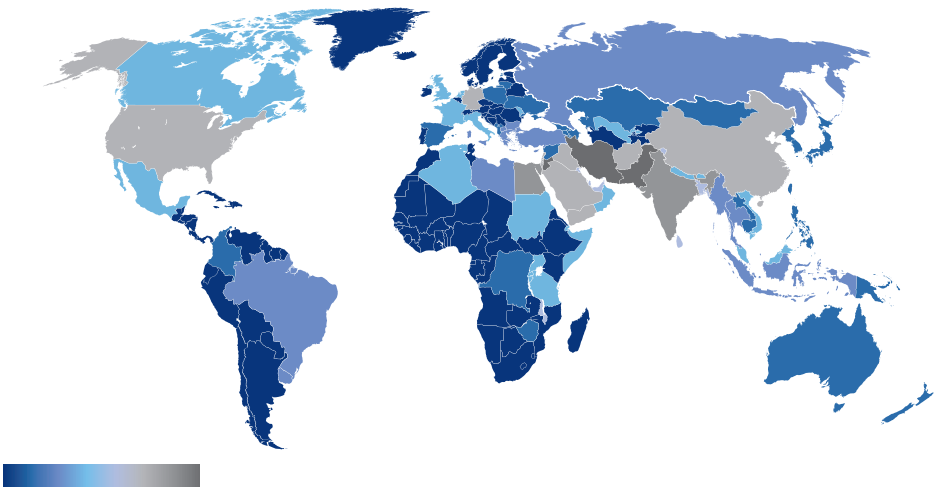


Рис. 13. Глобальная география электронной слежки АНБ США

Примечание: от темно-синего цвета к темно-серому — степени активности по нарастающей АНБ США в сфере электронного шпионажа в отношении той или иной страны.

Источник: The Guardian

- глобальный характер — кампании АНБ и британских спецслужб охватили одновременно многие десятки стран мира, включая членов и союзных блоков НАТО, и дружественных коалиций;
- массовость — вероятно, впервые в истории сбор персональных данных и слежка за гражданами вообще утратили избирательность. Гражданин стал объектом электронного наблюдения по умолчанию в результате развития технологий и инфраструктуры, необходимых для работы с *Big Data*;
- незаметность — технологический арсенал АНБ позволял годами собирать данные десятков миллионов пользователей, включая политических лидеров других стран, успешно сохраняя все в тайне до лета–осени 2013 г.;
- безопасный характер — несмотря на имиджевые и политические потери, США не потеряли ни одного агента, равно как и технику, в результате разоблачений Сноудена, благодаря трансграничной природе Интернета, не требующей присутствия людей «на месте».

Таблица 6. Ключевые разоблачения Эдварда Сноудена

№	Название/эпизод	Краткая информация о функционале
1	**Программа Bullrun**	С 2000 г. велось систематическое сотрудничество АНБ США с американской индустрией криптографии (шифрования) в целях внедрения недекларированных возможностей и функций (закладок, бэкдоров) в выпускаемые на национальный и глобальный рынок программные и аппаратные продукты для бизнеса, государственных учреждений и конечных пользователей, в том числе иностранных. В планах АНБ на 2013 г. — дальнейшее развитие успехов в сфере прежде всего аппаратного шифрования
2	**Эксплуатация АНБ фундаментальных уязвимостей в криптографических стандартах и алгоритмах (AES, OpenSSL)**	С 2011 г. — взлом протокола шифрования SSL, составляющего основу безопасности большинства коммуникаций в Сети, создание единой базы данных для мгновенного подбора криптоключей к зашифрованным данным. Длительная эксплуатация критической уязвимости в криптографическом пакете OpenSSL — Heartbleed, которой были подвержены до 66% всех веб-сайтов в мире
3	**Программа Follow the money и база данных «Тракфин»**	Систематическая слежка как минимум с 2012 г. за транзакциями физических и юридических лиц через платежную систему VISA и межбанковскими транзакциями через международную систему SWIFT. АНБ как минимум с 2012 г. обеспечило себе доступ к сетям системы SWIFT, через которую проходят 3 млрд операций в месяц. Целевые регионы отслеживания операций — Африка, Ближний Восток и Европа
4	**Программа PRISM**	Запущена в 2007 г., позволяет скачивать закрытую информацию с серверов интернет-гигантов США (включая Microsoft, Yahoo!, Google, Facebook, AOL, Skype, YouTube, Apple и PayPal). Доступ АНБ, ЦРУ и ФБР к данным частной e-mail-переписки, чатов, фото- и видеоматериалов, голосового трафика (VoIP), передаваемых через Сеть файлов, видеоконференций, введенных логинов и паролей, записей и действий в социальных сетях. Отслеживание звонков абонентов крупнейших сотовых операторов США внутри страны и по миру
5	**Программа XKeyscore**	Перехват содержимого ящиков электронной почты, списков почтовых контактов. При вводе IP-адреса — выявление всех посещенных веб-сайтов, введенных паролей, просмотренных документов; взлом аккаунтов в социальных сетях, доступ к переписке в онлайн-чатах и проч. Работу программы обеспечивали 700 серверов, частично размещенных в зарубежных посольствах и консульствах США, включая сервер в Москве

Окончание таблицы 6

№	Название/эпизод	Краткая информация о функционале
6	**Кибероперации спецслужб США в сетях иностранных государств, включая КНР, Иран, КНДР и Россию**	На операции в зарубежных информационных сетях в 2013 г. было предусмотрено 4,3 млрд долл. США. В 2011 г. была осуществлена 231 проактивная операция, цели которых в том числе включали «предотвращение распространения ядерного оружия» (одновременно в Натанзе был обнаружен Stuxnet)
7	**Перехват сеансов коммуникации иностранных политических лидеров**	Серия операций АНБ и британского Центра правительственной связи (GCHQ), в числе целей — зарубежные лидеры, включая Президента России Д.А. Медведева, президента Мексики Фелипе Кальдерона, президента Бразилии Дилмы Руссеф и федерального канцлера ФРГ Ангелы Меркель в 2009–2013 гг.
8	**Программа Tempora и ее составляющие — Mastering the Internet и Global Telecoms Exploitation**	Систематический сбор британским Центром правительственной связи (GCHQ) данных телефонных разговоров и интернет-трафика тысяч абонентов; полученные данные могли храниться до трех дней, метаданные — до 30 дней. Запись телефонных звонков, e-mail-переписки, записей и личных данных в Facebook
9	**Шпионаж АНБ за коммерческими структурами в Бразилии и других странах**	Взлом корпоративных сетей и прослушка высшего менеджмента крупнейшей бразильской нефтяной компании Petróleo Brasileiro S.A., венесуэльской нефтяной компании PdVSA
10	**Программы АНБ США RAMPART-A, Optic Nerve**	Сбор данных о коммуникациях пользователей по всему миру за счет прямого доступа к магистральной оптоволоконной инфраструктуре. Доступ к данным пользователей напрямую за счет врезок в магистральные оптоволоконные интернет-кабели. Обработка АНБ потока данных мощностью до 3 Тб/сек. Партнеры программы — более 30 стран, включая Данию и Германию

В плане положительных последствий разоблачения Сноудена стимулировали новый виток дискуссии о необходимости выработки международных норм ответственного поведения государств в Сети.

Кроме того, в центре внимания технического сообщества оказался вопрос о первопричинах столь тотальной слежки в Интернете, организованной АНБ и его британскими коллегами. Глобальная сеть с точки зрения ее архитектуры, технологических средств и форм

государственного регулирования традиционно считалась оптимальной площадкой для безопасной анонимной коммуникации. Конечно, разрастающиеся кампании кибершпионажа, хакерские атаки и все более активная политика государства в Сети способствовали корректировке этой оценки и до разоблачений Сноудена. Однако именно события 2013 г. показали широкой общественности, что в отношении пользователей и их персональных данных Интернет стал *стеклянным домом*, практически полностью проницаемым для спецслужб.

В результате вопрос, вставший два года назад перед техническим сообществом, может быть сформулирован так:

- «Является ли феномен масштабного государственного шпионажа в Сети *случайным сбоем* или *системным пороком* нынешней модели управления Интернетом?»
- И если речь идет о системном пороке архитектуры Интернета и управления им, «Какие технические и институциональные шаги помогут исправлению ситуации?».

Несмотря на то что на данный момент окончательный ответ на эти вопросы так и не представлен международному сообществу и интернет-пользователям, спустя два года с начала разоблачений Сноудена версия, согласно которой глобальные программы электронной слежки являются случайной аберрацией и не зависят от существующих пороков архитектуры безопасности Сети, выглядит все более сомнительной.

Многие эксперты как в техническом сообществе, так в частном секторе склонны рассматривать глобальную электронную слежку именно как системный порок, возникший в результате стремительного технического прогресса и глобализации Интернета, которыми не могли не воспользоваться спецслужбы различных государств. С учетом постоянного возникновения новых очагов нестабильности по всему миру, которые так или иначе позволяют спецслужбам технологически развитых государств обосновать пристальную массовую слежку за пользователями, компаниями и правительственными органами, возникает вопрос — какие технические, правовые и институциональные шаги могут сбалансировать интересы обеспечения национальной/глобальной безопасности с правом граждан на тайну частной жизни?

Признание системной проблемы в механизме управления Сетью может повлечь далеко идущие последствия на архитектурном

и техническом уровне, включая уровень технической инфраструктуры Сети и интернет-протоколы. Речь в том числе идет об изменении параметров и средств защиты от перехвата пакетов данных за счет обновления наиболее распространенных протоколов уровня приложений и транспортного уровня (HTTP, TCP/IP и проч.), а также стандартов шифрования трафика в Интернете. Подобные предложения звучали в рамках заседания рабочей группы по проектированию Интернета (IETF) в ноябре 2013 г. в г. Ванкувер, Канада.

Несмотря на то что с начала разоблачающей кампании Сноудена прошло более двух лет, поставленные вопросы до сих пор не получили исчерпывающего ответа. Представляется, что для его решения необходимо провести экспертную работу с привлечением членов технического сообщества, рассмотренных в разделе VI (IAB, IETF, IANA, ISOC, W3C и проч.). Площадка для такой работы может быть создана в рамках форума по вопросам управления Интернетом и инициативы его усиления и реформирования, а деятельность вестись в рамках процесса подготовки Договора о принципах управления Интернетом. При постоянном исполнительном секретариате IGF может быть создана экспертная комиссия по исследованию фундаментальных уязвимостей архитектуры Сети и модели управления ей.

Важно обеспечить участие в работе подобного механизма наряду с техническими экспертами представителей государств, — в частности, стран, пострадавших от деятельности АНБ и британского Центра правительственной связи (что совсем не исключает возможности участия в работе такой комиссии представителей США и Великобритании).

Если рассматриваемый формат взаимодействия технических экспертов окажется плодотворным, на выходе могут быть востребованы рекомендации практического характера, связанные со снижением уязвимости Сети и сужением технического окна возможностей по осуществлению массового сбора персональных данных в Сети.

На сегодняшний день, вне зависимости от возможных выводов технических экспертов, можно выделить ряд направлений, работа по которым может помочь уменьшению объема массовой слежки в Интернете:

- уже отмеченная представителями технического сообщества необходимость усиления защиты трафика на уровне наиболее часто используемых интернет-протоколов. Одна из реша-

емых задач в этой сфере — добиться шифрования по умолчанию максимальной доли интернет-трафика, передаваемого в Сети, за счет обновления параметров одного из наиболее распространенных протоколов уровня приложений (HTTP/2). Систематическая работа в этом направлении ведется с 2013 г. рабочей группой HTTP-bis в рамках IETF, а 17 февраля 2015 г. проект предлагаемого стандарта второй версии протокола был опубликован руководящей группой по проектированию Интернета (IESG);

- устранение фундаментальных уязвимостей в наиболее распространенных алгоритмах и стандартах криптографии (SSL, RSA), которые были «скомпрометированы» спецслужбами. На региональном уровне речь может идти и о продвижении полностью «нетрадиционных» СЗИ, таких как система российских стандартов шифрования ГОСТ, уже получившая импульс к наращиванию экспортного потенциала (в частности, в страны арабского мира);
- стимулирование развития сетевых коммуникаций на основе новых технологических решений, в том числе сетей, способных работать как в рамках Интернета, так и в обход него (сети Mesh, P2P и т. д.). Также могут рассматриваться варианты развития инструментов анонимизации наподобие TOR, однако исключительно при условии нивелирования их криминогенного потенциала (вопрос, выходящий за рамки компетенции технических экспертов).

Одна из требующих поддержки мер на уровне взаимодействия государства и бизнеса — развитие формата корпоративных «отчетов о прозрачности» (англ. *Transparency Reporting*). Одной из компаний, задавших сам формат отчета о прозрачности, стал Google, впервые опубликовавший такую отчетность в 2009 г. Одноименный и почти идентичный по формату продукт в 2011 г. выпустил Twitter, а в марте 2013 г. компания Microsoft опубликовала собственный Law Enforcement Report. Однако действительно широкое распространение практика Transparency Reporting получила именно после первой волны разоблачений Сноудена в 3–4 кв. 2013 г. В августе 2013 г. Глобальный отчет по государственным запросам (Global Government Requests) впервые выпустила сеть Facebook, в сентябре того же года свой отчет о прозрачности опубликовала Yahoo!.

Стремление крупнейших игроков сектора нивелировать репутационные риски, возникшие в результате разоблачений Сноудена, привело к тому, что отчет о прозрачности, по сути, превратился в новый стандарт отчетности в интернет-отрасли.

Кроме того, с конца 2013 г. к практике публикации отчетов о прозрачности стали подключаться и компании телекоммуникационного сектора, сперва американские (AT&T, Verizon), чуть позднее — британские (Vodafone). Причины по большей части были теми же самыми — новые разоблачения масштабных программ сотрудничества со спецслужбами США и Великобритании нанесли серьезный ущерб репутации западных телекоммуникационных гигантов.

Добровольное раскрытие корпорациями информации, отражающей статистику запросов государственных структур различных стран на предоставление данных интернет-пользователей, а также статистику реагирования на такие запросы со стороны компаний, само по себе не обеспечивает пользователям защиту от действий спецслужб. Но тем не менее такая деятельность повышает осведомленность пользователей о защите и обработке их данных, и стимулирует более активную позицию гражданского общества по данному вопросу. В течение 2013–2014 гг. предметом юридических споров между компаниями и государством стала частичная деклассификация и право первых на публикацию в отчетах точных цифр, отражающих статистику запросов секретных служб и судов (ранее публикация таких данных была запрещена). В настоящее время некоторые компании также публикуют данные о запросах на блокирование и удаление контента на основании претензий правообладателей на определенной территории, а также статистику интернет-трафика (Google, Twitter, Yahoo!).

Сегодня практика Transparency Reporting наглядно высвечивает устойчивый рост интереса государств к данным пользователей. Согласно отчету Google за январь–июнь 2014 г. число правительственных запросов выросло на 15% в первой половине 2014 г. и на 150% в течение последних пяти лет. Однако тот факт, что задокументированные в них данные об официально оформленных запросах — лишь верхушка айсберга в глобальном масштабе доступа спецслужб к данным пользователей этих и прочих сервисов, несколько обесценивает их значение.

Наконец, на международно-политическом уровне перед государствами и другими заинтересованными сторонами стоит несколько задач:

- Сокращение потенциала глобальной слежки в Сети на технологическом уровне. Требуется проработать возможности ограничения оборота и криминализации ПО, посредством которого осуществляется электронный сбор данных. Такие меры в принципе могут охватить далеко не весь спектр возможностей АНБ. Однако вместе с тем «шпионское» ПО (ПО для прослушивания голосовых коммуникаций, кейлоггеры, оборудование программ PRISM и Optic Nerve), не всегда причисляемое к вредоносному, составляет отдельную рыночную нишу. Однако эффективное регулирование и сокращение этой ниши возможно лишь при условии, что для этого будут задействованы механизмы международного сотрудничества, опирающиеся на международно-правовые механизмы.
- Однако до конца 2014 г. ни одна из попыток должным образом закрепить недопустимость массового шпионажа и нарушения права на тайну частной жизни в Сети не дала убедительного результата. На форуме NETmundial в апреле 2014 г. вопрос не получил должного внимания в финальной резолюции, хотя был основным стимулом к самой организации форума. Ни параграф в итоговом документе NETmundial, ни Резолюция ГА ООН A/RES/68/167 от 18.12.2013, во-первых, не обладают обязательной юридической силой, а во-вторых, не предлагают конкретных мер ответственности государств за осуществляемые ими действия в части массовой слежки в Сети.

В этой связи одним из перспективных вариантов видится распространение на программно-аппаратное обеспечение слежки и технологии его разработки механизмов Вассенаарских договоренностей по экспортному контролю за обычными вооружениями и товарами и технологиями двойного применения (ВД). На сегодняшний день участниками Вассенаарской договоренности, подписанной в 1996 г., являются 40 государств, включая США, Россию и большинство стран ЕС — т. е. весьма значительная часть ведущих разработчиков и распространителей информационных технологий «двойного назначения». Конкретным шагом в этом русле могло бы стать формирование реестра или банка данных программного

и аппаратного обеспечения (в том числе образцов исходного кода ПО), которое может быть использовано для тайного сбора данных пользователей в Сети или иных форм электронной слежки.

Также в рамках механизмов международно-правового института ответственности в случае повторения эпизодов, аналогичных тем, что были раскрыты Сноуденом в 2013 г., могла бы быть проработана возможность использования механизмов международных санкций. В случае достаточной консолидации международного сообщества, в новой резолюции ГА ООН можно сформулировать рекомендательные критерии и условия применения коммерческих, процессуальных и (или) иных санкций против государства, уличенного в массовом электронном шпионаже.

В числе потенциальных критериев, которые, как видится, могли бы обусловливать применение санкций, можно упомянуть:

- Несомненное нарушение права на тайну частной жизни, выраженное в характере собираемых данных (персональные данные, частная переписка и т. д.), за исключением метаданных; в отношении государств и организаций — сбор сведений, имеющих конфиденциальный характер, коммерческую, служебную либо государственную тайну.
- Массовый, неизбирательный характер слежки в Сети (собираются данные не отдельных лиц, а больших групп, либо сбор данных ведется вообще неизбирательно (*тотальный* шпионаж)).
- Глобальная угроза безопасности — т. е. государство в своей деятельности выходит за рамки своих национальных границ, собирает данные граждан, компаний и иных субъектов в нескольких или многих государствах сразу.
- Систематический характер деятельности — речь не идет о разовой акции, которая может быть продиктована случайным либо ошибочным мотивом; шпионаж и сбор персональных данных ведутся на постоянной либо долгосрочной основе; для сбора данных создается специальная инфраструктура.
- Отсутствие чрезвычайных обстоятельств, оправдывающих массовую электронную слежку с правовой точки зрения. Определение таких обстоятельств в терминах права — непростая задача; показателен как раз пример США, ведь программы АНБ, вызвавшие бурю негодования даже у ближайших союзников Вашингтона, с точки зрения самого американского законодательства по большей части вполне легитимны.

После терактов 11 сентября 2001 г., когда была очевидна острая угроза национальной безопасности, возникла срочная потребность в получении информации, которая помогла бы предотвратить возможные дальнейшие теракты и атаки. Косвенно к тотальной слежке американских спецслужб в Интернете привел принятый в октябре 2001 г. Патриотический акт (US PATRIOT Act), а именно секция 215, расширяющая полномочия спецслужб в плане массового сбора метаданных, который за десять лет стремительно эволюционировал. Поправка 2008 г. (FISA Amendment Act) вывела эти полномочия за пределы территории США при условии их применения к неамериканцам; технические же средства сбора данных лишь прогрессировали с развитием интернет-сервисов. Таким образом, с точки зрения законодательства США, программы спецслужб, раскрытые Эдвардом Сноуденом, оставались легитимными. Однако 1 июня 2015 г. срок действия секции 215 истек, и Конгресс вынужден был решать, как заменить механизмы сбора данных и полномочия спецслужб, возникшие в эру президентства Джорджа Буша-младшего, и есть ли в этом необходимость. За реформирование Акта о патриотизме выступали крупнейшие интернет-корпорации, чей бизнес зависит от уверенности пользователей в приватности их коммуникаций и соразмерности действий спецслужб по обеспечению национальной безопасности. С учетом растущей угрозы терроризма, активизации Исламского государства (ИГИЛ — запрещено в России) и других очагов нестабильности в различных регионах, существовала вероятность того, что действие закона будет продлено до конца 2019 г. Однако этого не случилось, взамен был принят повторно внесенный в Конгресс USA FREEDOM Act, т. н. «Акт о свободе». В числе прочих положений нового закона явно прописан запрет на принятие норм, вновь разрешающих массовый сбор спецслужбами метаданных пользователей; запрет вступает в силу через 180 дней после принятия Акта о свободе. Таким образом, авторы закона позаботились о том, чтобы статья 215 Акта о патриотизме не «возродилась» вновь усилиями президентской администрации. Однако многочисленные критики Акта о свободе утверждают, что в реальности массовый сбор данных американских граждан все же будет продолжаться на основании статьи 702 поправок 2008 г. к Акту о наблюдении

за иностранной разведкой от 1978 г. В целом вопрос о наличии правовых оснований и реальном продолжении электронного шпионажа АНБ и другими правительственными агентствами США и ряда других стран остается открытым.

Однако деятельность, затрагивающая интересы и права государств и пользователей по всему миру, не должна регулироваться исходя из интересов национальной безопасности одного или нескольких государств.

- Ответственность политического руководства государства за данные действия. Речь идет о тех случаях, когда акты электронного шпионажа не являются произволом отдельных исполнителей в спецслужбах, а планируются и санкционируются на том уровне принятия решений, который предполагает осведомленность политического руководства государства.

В практическом смысле едва ли уместно прорабатывать возможности применения мер воздействия по подобным основаниям в рамках СБ ООН. Однако возможная резолюция ГА ООН может послужить «модельным текстом» для региональных организаций, в том числе ЕС, Совета Европы, ОБСЕ, АСЕАН. В этом случае можно рассматривать возможность согласования и применения против государства, ведущего глобальный шпионаж в Интернете, таких санкций, как ограничение сотрудничества в сфере ИКТ и эмбарго на отдельные виды ИТ-продукции. Также представляется возможной с правовой точки зрения проработка различных опций процессуальных санкций, таких как приостановка членства и (или) иных полномочий государства в соответствующей международной организации.

Обсуждение подготовки такой резолюции ГА ООН могло бы состояться на площадке ГПЭ ООН или же всемирного Форума по управлению Интернетом.

Дополнительная информация

1. Куликова А. Отчет о прозрачности и политика конфиденциальности ИКТ-корпораций до и после разоблачений Сноудена // Электронный бюллетень ПИР-Центра «Пульс кибермира». 2014. № 1 (108). URL: http://www.pircenter.org/articles/1691-transparency-reporting-and-confidentiality-policies-of-ict-corporations-before-and-after-snowden (дата обращения: 01.03.2016).

2. Куликова А. Магистерская диссертация «The Importance of Being Transparent: Looking at the ICT Companies' Transparency Reports Through the Prism of the NSA Surveillance Leak», Лондонская школа экономики и политических наук (LSE), 30.08.2013. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2429707 (дата обращения: 01.03.2016).

Документы

1. IETF 88 Proceedings. Vancouver, CA 2013-11-03. Internet Engineering Task Force. URL: https://www.ietf.org/proceedings/88/ (дата обращения: 01.03.2016).
2. Резолюция Генеральной Ассамблеи ООН от 18.12.2013 A/RES/68/167 «Право на неприкосновенность личной жизни в цифровой век». URL: http://www.un.org/ru/documents/ods.asp?m=A/RES/68/167 (дата обращения: 01.03.2016).
3. Отчет о государственных запросах. Веб-сайт Facebook, 2015. URL: https://govtrequests.facebook.com/ (дата обращения: 01.03.2016).
4. Transparency Report. Communicate fearlessly to build trust. Веб-сайт Twitter. URL: https://transparency.twitter.com/ (дата обращения: 01.03.2016).
5. Access to information. Data that sheds light on how laws and policies affect Internet users and the flow of information online. Веб-сайт Google Inc. URL: http://www.google.com/transparencyreport/ (дата обращения: 01.03.2016).
6. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Official website. URL: http://www.wassenaar.org/ (дата обращения: 01.03.2016).

Раздел VIII

Мы признаем исключительно важную позитивную роль, которую играет Интернет в мире в плане содействия экономическому, социальному и культурному развитию. Мы считаем важным вносить вклад и участвовать в мирном, безопасном и открытом киберпространстве, и мы подчеркиваем, что безопасность при использовании информационных и коммуникационных технологий (ИКТ) с применением универсально признанных норм, стандартов и практик имеет первостепенную важность.

Этеквинская декларация и Этеквинский план действий
(приняты по итогам Пятого саммита БРИКС 27 марта 2013 г.)

Мы согласны с тем, что необходимо сохранять ИКТ, и в частности Интернет, как инструмент мира и развития и не допускать их использования в качестве оружия. Кроме того, мы обязуемся сотрудничать друг с другом в выявлении возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования ИКТ. <...> Учитывая значимость этих вопросов, мы отмечаем российское предложение о совместной разработке соглашения между странами БРИКС о сотрудничестве в данной области.

Форталезская декларация
(принята по итогам Шестого саммита БРИКС 15 июля 2014 г.)

Страны БРИКС как участники глобальной дискуссии по вопросам управления Интернетом и МИБ

Сегодня страны БРИКС образуют один из наиболее обширных и быстрорастущих сегментов Глобальной сети. По состоянию на ноябрь 2015 г. интернет-аудитория стран БРИКС насчитывала более 1,3 млрд пользователей (более 40% мировой аудитории) с темпами роста от 10 до 41% ежегодно. Индия и Бразилия стали глобальными лидерами по темпам прироста интернет-аудитории в 2013 г. (31 и 37% соответственно). Вклад интернет-сектора в экономики стран форума уже превысил 500 млрд долл. США, в обозримом будущем также прогнозируется быстрый рост этого показателя.

Таблица 7. Статистика использования Интернета и основные демографические показатели в странах БРИКС

Страна	Население по состоянию на март 2014 г. (тыс. чел.)	Количество интернет-пользователей на июнь 2013 г. (тыс. чел.)	Место в мире по количеству интернет-пользователей	Доля проникновения Интернета на июнь 2013 г., (%)	Доля от мировой интернет-аудитории, (%)
Бразилия	201 032	99 358	5	49,4	4,13
Индия	1 242 580	151 599	3	12,2	6,30
КНР	1 363 780	568 192	1	41,7	23,62
Россия	143 666	75 926	6	52,8	3,16
ЮАР	52 981	20 012	25	37,8	0,83
БРИКС	**3 004 039**	**915 087**	**...**	**38,8**	**38,01**

Примечание: при составлении таблицы были использованы следующие источники информации:

1. Раздел «Государства и территории, ранжированные по численности населения: 2012 г.». Официальный сайт Бюро переписи населения США, www.census.gov
2. Оценка населения Бразилии по состоянию на 1 июля 2013 г. Сайт Бразильского института географии и статистики, www.ibge.gov.br
3. Раздел «Счетчик населения». Сайт Indiastat.com компании Datanet India Pvt. Ltd
4. Раздел «Официальный счетчик населения Китая». Официальный сайт Национального бюро статистики Китая (National Bureau of Statistics of China), www.data.stats.gov.cn
5. Оценка численности постоянного населения на 1 января 2014 г. и в среднем за 2013 г. Официальный сайт Федеральной службы государственной статистики России, www.gks.ru
6. Промежуточная оценка численности населения в 2013 г. Официальный сайт Службы статистики ЮАР (StatSA), www.statssa.gov.za
7. Портал Internet World Stats, www.internetworldstats.com

В ближайшем будущем население БРИКС станет самым многочисленным и активным сегментом глобального информационного общества.

Вместе с тем до последнего времени государства БРИКС преимущественно не проявляли себя в качестве организованной международной коалиции, имеющей и продвигающей согласованную повестку дня в вопросах безопасности в сфере ИКТ и управления Интернетом на ключевых международных площадках. В рамках площадок ВКМЭ в 2012 г., NETmundial 23–24 апреля 2014 г., IGF в Стамбуле 10–13 ноября 2015 г. и других глобальных встреч за последние годы не были представлены конкретные инициативы и согласованные позиции стран БРИКС по ключевым вопросам в повестке дня. В частности, речь идет:

- о завершении процесса по передаче контроля над исполнением функций IANA;
- об обеспечении «сетевой нейтральности» на уровне нормативного регулирования и саморегулирования в страновом и международном масштабе;
- о пресечении и предупреждении массированной слежки в Сети;
- о поиске институционального баланса между интересами государств и иных заинтересованных сторон в рамках формирования перспективной функциональной модели управления Интернетом.

Пассивность государств форума в данных вопросах, очевидно, обусловлена относительно слабой проработкой вопросов в сфере ИКТ в рамках БРИКС по сравнению с содержанием ее традиционной «корзины» — реформой глобальных финансовых институтов. Результатом является недостаточное вовлечение структуры, объединяющей в своих границах 38% интернет-пользователей, в проработку критически важного и самого динамичного измерения современных глобальных процессов и трансформации глобальных институтов — управления Интернетом.

Кроме того, вопросы ИКТ в контексте реформы глобальных институтов могут служить внутреннему укреплению самой БРИКС в качестве одной из основных граней идентичности и совместной повестки дня для стран форума. Работа над трансграничными вопросами управления Интернетом и ИКТ-безопасностью нивелирует ключевые слабости БРИКС, такие как региональные конфликты

интересов и несовпадение приоритетов повестки дня в зависимости от их территориальной привязки.

Наконец, в вопросах развития Интернета БРИКС несет значительный потенциал лидерства, будучи одним из наиболее крупных, организованных и активных форматов, агрегирующих и выражающих интересы незападного мира. Сегодня ряд факторов — экономических, демографических, политических и имиджевых (связанных с разоблачением государственных программ слежки в Интернете в 2013 г.) способствует формированию запроса на изменение глобального баланса лидерства в формировании и продвижении повестки дня по широкому кругу вопросов, связанных с ИКТ и Интернетом — от свободы слова в Сети до проблем расширения доступа в регионах с низкими уровнями доходов и защиты права на тайну частной жизни в Сети. Общей чертой для этого процесса является рост потребности в выражении и отстаивании интересов стран развивающегося мира, слабо участвовавших в управлении Интернетом ранее. Страны БРИКС могут использовать этот процесс, более активно реализовать свой потенциал в широком спектре вопросов управления Сетью.

Первые значительные практические шаги в этом направлении имели место на VI саммите БРИКС в г. Форталеза, Бразилия, прошедшем 15–16 июля 2014 г., где были озвучены конкретные инициативы, прежде всего в области МИБ (см. табл. 8).

Таблица 8. Итоги шестого саммита БРИКС 2014 г. применительно к вопросам МИБ и управления Интернетом

Группы вопросов	Достигнутые договоренности, согласованные позиции
МИБ	Обязательство сотрудничать в выявлении возможностей для осуществления совместных действий по решению общих проблем безопасности в сфере использования ИКТ. Необходимость выработки универсального и юридически обязательного международно-правового документа для борьбы с киберпреступностью на площадке ООН. Необходимость сохранять ИКТ, и в частности Интернет, как инструмент мира и развития и не допускать их использования в качестве оружия. Поддержка российского предложения о разработке соглашения между странами БРИКС о сотрудничестве по вопросам обеспечения безопасности в области использования ИКТ
Управление Интернетом	Осуждение актов массовой электронной слежки и сбора данных о частных лицах по всему миру, а также нарушения суверенитета государств и прав человека, в частности права на неприкосновенность частной жизни

В дополнение к форталезским инициативам прослеживается возможность закрепления и наращивания роли государств форума в проработке ключевых вопросов МИБ и управления Интернетом по следующим направлениям.

- Опыт США и России, а также наработки на площадках ОБСЕ и АСЕАН говорят о том, что в среднесрочной перспективе важным направлением сотрудничества в рамках БРИКС может стать выработка многосторонних механизмов мер доверия в области ИКТ и их использования в сфере международной безопасности. Первые шаги в этом направлении уже были сделаны в рамках подготовки и проведения саммита БРИКС в Уфе в 2015 г. Так, в ходе заседания Рабочей группы экспертов государств — участников БРИКС по вопросам безопасности в сфере использования ИКТ, которое состоялось в Москве 16–18 июня 2015 г., российская сторона представила рабочий проект межправительственного соглашения БРИКС о сотрудничестве в области обеспечения безопасности в сфере использования ИКТ.
- В Уфимской декларации БРИКС, принятой по итогам VII саммита форума, содержится призыв к международному сообществу «сосредоточить свои усилия на мерах укрепления доверия, создании потенциала, неприменении силы и предотвращении конфликтов в области использования ИКТ». Кроме того, документ относит к числу задач рабочей группы экспертов проработку вопросов сотрудничества между странами БРИКС с использованием центров реагирования на инциденты компьютерной безопасности (CSIRT), укрепления потенциала, а также разработки международных норм, принципов и стандартов. Однако конкретные предложения в части мер доверия в области использования, сопоставимые с механизмами, наработанными в рамках ОБСЕ и двустороннего трека РФ–США, на площадке БРИКС пока не выработаны. Создание и закрепление в долгосрочной повестке дня БРИКС может быть актуальной задачей в горизонте саммита 2016 г., а также в последующей среднесрочной перспективе.
- Страны БРИКС могут оказать поддержку и придать импульс инициативе создания на базе IGF площадки по проработке глобального соглашения о принципах управления Интернетом, озвучивая и продвигая такую инициативу в рамках процесса ВВУИО +10, саммитов IGF и собственной площадки. Также страны форума потенциально могли бы выступить с инициа-

тивой размещения на своей территории (Бразилия, ЮАР, Индия) технического и административного обеспечения работы постоянного секретариата, координирующего подготовку глобального соглашения, что отразило бы растущую роль развивающихся стран в вопросах управления Сетью.

- Государства БРИКС могли бы содействовать учреждению и запуску работы комиссии по исследованию фундаментальных уязвимостей архитектуры глобального управления Интернетом в рамках исполнительного секретариата IGF или другой площадки с участием всех заинтересованных сторон. Работа комиссии может иметь целью подготовку Доклада с рекомендациями по данному вопросу широкому кругу политических руководителей и глобальному интернет-сообществу (рабочая группа по проектированию Интернета (IETF), ICANN, Общество Интернета (ISOC), Архитектурный совет Интернета (IAB) и др.).
- Наращивание сотрудничества стран форума в части реализации совместных инфраструктурных проектов в сфере интернет-коммуникаций и ИКТ. Целесообразно скорейшее завершение прокладки трансконтинентального «кабеля БРИКС» как для диверсификации магистральной оптоволоконной инфраструктуры Сети, так и в целях расширения широкополосного доступа в странах форума и сопредельных регионах (Индия, ЮАР, южная часть Африки).
- Иные совместные проекты могут включать в себя разработку продуктов в нише открытого ПО (open-source software), в том числе ОС, коммерческих приложений, интерактивных образовательных онлайн-платформ, электронных площадок оказания государственных услуг и т. д. Также речь может идти о совместных проектах разработки средств защиты информации (СЗИ), включая коммерческие продукты в нише шифрования и криптографии. Активное сотрудничество в этой сфере может, в свою очередь, подтолкнуть оптимизацию законодательств ряда государств форума в части продвижения национальных продуктов в нише СЗИ на внешние рынки (включая российские наработки в области шифрования данных на основе стандартов ГОСТ).
- Вопросы безопасности в сфере использования ИКТ в рамках БРИКС могли бы, как отмечалось выше, получить развитие в рамках формата многосторонних мер доверия между членами форума. Первоначальные шаги могут заключаться в разработке

Рис. 14. Проект трансконтинентального морского магистрального оптоволоконного кабеля БРИКС

Примечание: проект предполагает прокладку оптоволоконного кабеля длиной 32 000 км от Владивостока до бразильской Форталезы через Индию, Китай и ЮАР.

Источник: Rob Minto.

на площадке БРИКС рамочных двусторонних мер доверия и их принятия государствами форума (Индия–Россия, Россия–Китай, Индия–Бразилия, Россия–Бразилия и т. п.). К 2020 г. может быть поставлена цель конвертации накопленного в рамках форума опыта и капитала доверия в многосторонний формат, включающий все пять государств. Прикладными инструментами, которые также имеют перспективы в формате БРИКС, также видятся совместные киберучения стран форума с акцентом на отражение угроз объектам КИИ, а также укрепление взаимодействия между их CERTs/CSIRTs. В перспективе возможна организация круглосуточного пункта обмена данными о киберинцидентах и создание Координационного центра команд реагирования на компьютерные инциденты стран БРИКС (CC-BRICS CERT).

- Более активное аккумулирование и использование «внешней» поддержки своих позиций по вопросам ИКТ. В качестве потенциального примера можно упомянуть заявление с призывом БРИКС активизировать свое участие в дискуссии об управлении Интернетом, опубликованное Международной ассоциацией экспертов в области управления Интернетом Just Net

Coalition 15 июля 2014 г. к саммиту БРИКС в Форталезе. Результатом успешной реализации данных возможностей могло бы стать существенное укрепление БРИКС в качестве выразителя мнений развивающегося мира по вопросам управления Интернетом, а также повышение синергии от взаимодействия государств форума по широкому спектру вопросов ИКТ и их использования.

Дополнительная информация

1. Материалы досье журнала «Индекс безопасности» «БРИКС и передовые технологии: перспективы сотрудничества и интересы России» (авторы: Андрей Баклицкий, Евгений Бужинский, Олег Демидов, Павел Лузин) // Индекс безопасности. Зима 2013. № 4 (107). С. 85–88.
2. Демидов О.В. БРИКС в глобальном управлении Интернетом: Форталеза-2014 как новая точка отсчета? // Электронный журнал ПИР-Центра «Пульс кибермира». Июнь–август 2014 г. № 3 (10). URL: http://www.pircenter.org/articles/1705-briks-v-globalnom-upravlenii-internetom-fortaleza2014-kak-novaya-tochka-otscheta (дата обращения: 01.03.2016).

Документы

1. Форталезская декларация (принята по итогам шестого саммита БРИКС), г. Форталеза, Бразилия, 15.07.2014. Официальный сайт президента Российской Федерации. URL: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCIQFjAB&url=http%3A%2F%2Fwww.kremlin.ru%2Fmedia%2Fevents%2Ffiles%2F41d4f160607850ce6e9c.doc&ei=J7AGVbSCO8e_ygOsqYKoCw&usg=AFQjCNHozOL6krmoA2zosVCPHJL8V3WxKg&bvm=bv.88198703,d.bGQ&cad=rjt (дата обращения: 01.03.2016).
2. Этеквинская декларация и Этеквинский план действий. Официальный сайт президента Российской Федерации. 27.03.2013. URL: http://news.kremlin.ru/ref_notes/1430 (дата обращения: 01.03.2016).
3. Just Net Coalition statement to the BRICS Summit in Fortaleza, Brazil. Knowledge Commons. 16 July 2014. URL: http://www.knowledgecommons.in/2014/07/16/just-net-coalition-statement/ (дата обращения: 01.03.2016).

Аббревиатуры и сокращения, используемые в тексте

CCD COE — Центр передовых практик кибероборонь НАТО, Таллин, Эстония
CERT — Центр реагирования на компьютерные инциденты
CSIRT — Группа реагирования на инциденты компьютерной безопасности
DNS — Система доменных имен
GAC — Правительственный консультационный комитет при Корпорации Интернета по присвоению имен и номера (ICANN)
IAB — Совет по архитектуре Интернета
IANA — Администрация адресного пространства Интернет
ICANN — Корпорация Интернета по присвоению имен и адресов
IETF — Рабочая группа по проектированию Интернета
IGF — Форум по управлению Интернетом
ISOC — Общество Интернета
NTIA — Национальная администрация по телекоммуникациям и информации США
RFC — запрос на комментарии
RIR — Региональная регистратура Интернета
W3C — Консорциум Всемирной сети
АНБ — Агентство национальной безопасности США
АСЕАН — Ассоциация государств Юго-Восточной Азии
ВВУИО — Всемирная встреча на высшем уровне по вопросам информационного общества
ВКМЭ — Всемирная конференция по международной электросвязи
ВОИС — Всемирная организация интеллектуальной собственности
ВЭФ — Всемирный экономический форум
ГПЭ ООН — Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций ООН
КВО — критически важный объект
КИ — критическая инфраструктура
КИИ — критическая информационная инфраструктура
МАГАТЭ — Международное агентство по атомной энергии
МИБ — международная информационная безопасность
МСЭ — Международный союз электросвязи
МУС — Международный уголовный суд

НАТО — Организация Североатлантического договора
ОБСЕ — Организация по безопасности и сотрудничеству в Европе
ОДКБ — Организация Договора о коллективной безопасности
ОЭСР — Организация экономического сотрудничества и развития
ПО — программное обеспечение
РАЭК — Российская ассоциация электронных коммуникаций
РМЭ — Регламент международной электросвязи
ШОС — Шанхайская организация сотрудничества

Рабочая группа по международной информационной безопасности и глобальному управлению Интернетом при Экспертном совете ПИР-Центра

1. **Волчинская Елена Константиновна**, главный специалист, Юридический отдел, Федеральная нотариальная палата
2. **Демидов Олег Викторович**, консультант, ПИР-Центр
3. **Зинина Ульяна Викторовна**, директор по корпоративным вопросам, Microsoft Russia
4. **Зиновьева Елена Сергеевна**, доцент, кафедра мировых политических процессов, МГИМО МИД России
5. **Каберник Виталий Владимирович**, начальник отдела, Управление инновационного развития, МГИМО МИД России
6. **Касенова Мадина Балташевна**, заведующая кафедрой международного частного права, Дипломатическая академия МИД России
7. **Куликова Александра Владимировна**, менеджер по взаимодействию с заинтересованными сторонами в Восточной Европе и Центральной Азии, Корпорация Интернета по присвоению имен и номеров (ICANN)
8. **Левова Ирина Юрьевна**, директор по стратегическим проектам, Институт исследований Интернета
9. **Лукацкий Алексей Викторович**, бизнес-консультант по безопасности, Cisco, Москва, Россия (с 2014 г.)
10. **Пискунова Наталья Александровна**, руководитель проекта, Международный форум по ядерному страхованию
11. **Романов Андрей Георгиевич**, заместитель директора, Координационный центр доменов .RU/.РФ
12. **Сачков Илья Константинович**, генеральный директор, Group-IB

13. **Тодоров Леонид Львович**, генеральный менеджер, Ассоциация администраторов национальных доменов верхнего уровня Азиатско-Тихоокеанского региона (APTLD)
14. **Федоров Александр Валентинович**, член Экспертного совета, ПИР-Центр
15. **Черненко Елена Владимировна**, заведующая отделом внешней политики, Издательский дом «Коммерсантъ»
16. **Якушев Михаил Владимирович**, вице-президент по взаимодействию с заинтересованными сторонами в Восточной Европе и Центральной Азии, Корпорация Интернета по присвоению имен и номеров (ICANN)

Об авторе

Олег Демидов пришел в ПИР-Центр в 2011 г. и с тех пор работает в сфере управления Интернетом и информационной безопасности. В 2013–2014 гг. руководил программой ПИР-Центра «Глобальное управление Интернетом и международная информационная безопасность».

В ходе реализации этой программы ПИР-Центр стал ведущим российским неправительственным институтом, изучающим влияние Интернета и ИКТ на международные отношения и глобальную безопасность.

Олег Демидов принимал участие в крупнейших международных форумах и саммитах по вопросам управления Интернетом, включая конференции ICANN, саммит NETmundial, IGF, Глобальную конференцию по вопросам киберпространства 2015 г. и проч.

С 2015 г. Олег Демидов консультирует ПИР-Центр по вопросам дальнейшего развития программы, также состоит в Исследовательской консультативной сети при Глобальной комиссии по управлению Интернетом (GCIG), ведет исследовательское взаимодействие с ICANN и российским техническим сообществом.

О ПИР-Центре

ПИР-Центр, основанный в 1994 г., является ведущей в России неправительственной организацией, специализирующейся на изучении вопросов глобальной безопасности, ядерного нераспространения, международной информационной безопасности и глобального управления Интернетом.

С начала 2000-х гг. эксперты ПИР-Центра ведут исследования в сфере информационной безопасности. В 2001 г. вышла книга «Информационные вызовы национальной и международной безопасности», первое издание по данной теме в России. В 2011 г. создана программа ПИР-Центра «Глобальное управление Интернетом и международная информационная безопасность ("ГУИ и МИБ")». В 2013 г. в рамках программы вышел тематический номер журнала «Индекс безопасности» — «Глобальная безопасность в цифровую эпоху» — с докладами ведущих российских и зарубежных экспертов; выходит электронное издание «Пульс Кибермира» и научные доклады.

В исследовании вопросов управления Интернетом и влияния ИКТ на глобальную безопасность ПИР-Центр сотрудничает с российскими государственными органами, частным сектором, отечественным и глобальным техническим сообществом, а также международными организациями, включая структуры ООН (ЭКОСОС, ЮНИДИР, МСЭ). Эксперты ПИР-Центра участвуют в крупнейших российских международных встречах и форумах по вопросам, связанным с «ГУИ и МИБ», вносят вклад в развитие глобальных и региональных подходов к решению ключевых проблем в этой сфере.

Библиотека ПИР-Центра

Демидов Олег

Глобальное управление Интернетом и безопасность в сфере использования ИКТ

Ключевые вызовы для мирового сообщества

Руководитель проекта *А. Ефимов*
Арт-директор *Л. Беншуша*
Дизайнер *М. Грошева*
Корректор *И. Астапкина*
Компьютерная верстка *А. Абрамов*

Подписано в печать 06.07.2016. Формат 70×100 1/16.
Бумага офсетная № 1. Печать офсетная.
Объем 12,5 печ. л. Тираж 1000 экз. Заказ № .

ООО «Альпина Паблишер»
123060, Москва, а/я 28
Тел. +7(495) 980-53-54
www.alpina.ru
e-mail: info@alpina.ru

Знак информационной продукции
(Федеральный закон № 436-ФЗ от 29.12.2010 г.)

0+

Для заметок