ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕГОДНЯ: АЛОГИЗМЫ РАЗВИТИЯ

Главному редактору:

Только ленивый, рассуждая о новых угрозах в контексте постмодерна, не говорит об информационной безопасности. Но лишь немногие, за исключением разве что глубоких профильных специалистов, могут ответить на вопрос, что же такое информационная безопасность сегодня.

В преамбуле к свежему официальному документу уровня ООН одной из стран *Большой семерки* сказано: «Киберпространство играет ключевую роль в поддержании инновационной всепланетной экономики и обеспечения связи между обществами; оно позволяет предпринимательству свободно заниматься инновациями, снижением себестоимости и поиском доступа к новым рынкам. Логичные, последовательные и предсказуемые взаимодействия в киберпространстве помогут поддержать всепланетную инновационную цифровую экономику, энергичное, многообразное и подключенное всепланетное общество, укрепить международный мир и безопасность»[1]. Гораздо проще сказано в соглашении стран — членов Шанхайской организации сотрудничества (ШОС) о сотрудничестве в области информационной безопасности: «Информационная безопасность — состояние защищенности личности общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве»[2]. При этом второе определение, несмотря на кажущуюся простоту, ближе подходит к сути вопроса и в меньшей степени нуждается в пояснениях.

В начале 1990-х гг., когда термин *информационная безопасность*[3] только начал появляться в политологических работах, обозначаемая им сфера отношений понималась как антипод *информационной войны*. Отсюда и берет начало та несостыковка сути современного понятия информационной безопасности и того формального наполнения, которое иногда в это понятие вкладывается *по инерции*. Причем сама информационная война тогда определялась не иначе как в стилистике межгосударственного силового противоборства. Не исключалось, правда, что участниками конфликта могут быть и негосударственные акторы, но под ними в основном понимали противостоящие в вооруженной борьбе за власть внутренние политические силы. Тогда такие противоборства называли конфликтами, не относимыми к войне, зачастую имея в виду гражданские войны, борьбу за национальную независимость и автономию и тому подобное. Активными поборниками противодействия информационной угрозе тогда были, пожалуй, только США — да и то в основном в рамках национальных научных конференций.

Первые разработки в области военных информационных операций также осуществлялись в Соединенных Штатах, где уже начиная с 1993 г. стали готовиться

и публиковаться различного рода военные уставы, наставления, доктрины ведения информационных операций. В 1998 г. Комитет начальников штабов выпустил фундаментальный труд под названием «Объединенная доктрина информационных операций»[4], в котором информационная война получила свое практическое предметное описание. О значении интернета и социальных сетей для активного противоборства в информационном пространстве тогда, по понятным причинам, никто не задумывался, однако *психологические операции* — как тактические, так и стратегические — напрямую относили к информационной сфере.

Спустя годы, в 2004 г. представитель США в Группе правительственных экспертов ООН по международной информационной безопасности заявляла, что никакой угрозы информационной войны нет, а сама информационная война является ничем иным, как химерой. Основной угрозой, с точки зрения Вашингтона, следовало считать киберпреступность. И до сих пор после цветных революций, *Арабской весны* и выявления сложнейших вредоносных программных продуктов, направленных против объектов критической инфраструктуры, Вашингтон продолжает защищать эти же позиции, хотя и более гибко — наличие военной угрозы сегодня все же признается[5].

С тех пор болезнью обеспечения информационной безопасности в той или иной степени заразились многие страны и чуть ли не все международные организации. В настоящее время работает уже третья Группа правительственных экспертов ООН по международной информационной безопасности (ГПЭ МИБ). На протяжении 14 лет ежегодно Генассамблея ООН принимает резолюцию Первого комитета «Достижения в сфере коммуникации и информатизации в контексте международной безопасности», непосредственно посвященную этой проблеме. В течение трех лет по линии Третьего комитета продвигалась резолюция «Культура кибербезопасности». Вопросы информационной безопасности и информационного общества стали постоянными в повестке дня Международного союза электросвязи (МСЭ), под эгидой которого в два этапа, в 2003 и 2005 гг., прошел Всемирный саммит информационного общества — вероятно, самый масштабный форум современности в сфере информационной безопасности. Вопросы информационной безопасности и кибербезопасности значатся в списках важнейших для таких международных организаций, как ШОС, Организация по безопасности и сотрудничеству в Европе (ОБСЕ), Региональный форум Ассоциации государств Юго-Восточной Азии по безопасности (АРФ). Активно работают над военными аспектами данной проблемы НАТО и Организация Договора о коллективной безопасности (ОДКБ). Борьба с терроризмом уже давно не рассматривается иначе как в увязке с вопросами использования интернета в целях пропаганды, рекрутирования новых членов и организации терактов террористическими группами. С передовиц крупнейших СМИ не сходят вопросы киберпреступности. А уж точного числа конференций, симпозиумов, семинаров, круглых столов и иных мероприятий, так или иначе тематически привязанных к повестке информационной безопасности, не знает, вероятно, никто.

Последней каплей для непрофессиональной, но заинтересованной в вопросах информационной безопасности публики должны были бы стать сообщения об упомянутых вредоносных программах, таких как *Stuxnet*, *Duqu*, *Flame*, *Gauss*. Согласно имеющимся на сегодня данным, эти программы якобы способны работать в разных программных средах, распространяясь по интернету, и наносить серьезный физический ущерб вплоть до полного выведения из строя различных, в том числе критических и особо опасных объектов производства, транспорта, энергетики. Информационные системы управления критически важными инфраструктурами стали не только объектами защиты, но и целями для атак. Специалисты предвидели и осознавали эту угрозу еще 20 лет назад, но не смогли объяснить мировому сообществу, что противодействие ей требует, чтобы все информационное пространство (а не только сети связи и технико-программные продукты типа интернета) находилось под национальной и международной защитой.

Постепенно и политологам, и политикам становится ясно, что постиндустриальное общество нуждается не только и не столько в мирном атоме, сколько в мирном информационном пространстве. Договор о нераспространении ядерного оружия (ДНЯО) стал поворотным моментом в истории военной ядерной технологии, нанеся удар по историческому пессимизму и алармизму в международных отношениях. Конечно, заключить аналогичный договор в условиях постиндустриального общества уже вряд ли возможно, но противостояние информационной угрозе, тем не менее, по-прежнему требует многосторонних усилий аналогичного масштаба и глубины. Если это удастся сделать, можно будет констатировать, что человечество осознало бесперспективность насилия в международных отношениях.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — РАЗЛИЧНЫЕ ВЗГЛЯДЫ

Далеко не все сегодня понимают суть и постановку такой задачи одинаково. На сегодняшний день в общем дискурсе об обеспечении международной информационной безопасности четко прослеживаются три направления, которые с известной долей условности можно определить как либеральное, консервативное и прагматическое.

Защитники свободы интернета

В эту широкую группу сегодня попадает большинство интересующихся проблематикой информационной безопасности. Большую долю среди либералов составляет молодежь, в том числе та ее часть, которая в основном умеет только нажимать кнопки на клавиатуре. Теперь с появлением планшетников для многих из них и такое действие стало интеллектуально сложной задачей — достаточно просто провести пальцем по экрану, а вместо писем, которые надо писать, можно обмениваться фотографиями, сделанными при помощи тех же, как теперь все чаще говорят, *гаджетов*. Обмен информацией и доступ к ней видятся представителям данной группы именно в свете особенностей использования ими технологий. В любом случае представители группы либералов — это активные пользователи интернета, по роду своих основных занятий не связанные с деятельностью критических инфраструктур, армией, силовыми и правоохранительными структурами, вопросами, представляющими государственную тайну, и вообще с вопросами функционирования и безопасности государства. Группу объединяет приверженность одному тезису — глобальная сеть должна прежде всего обеспечивать свободу доступа к информации и свободу распространения информации.

О том, что такое информация, все они, как правило, не задумываются. В среде *защитников свободы интернета* считается, что безопасность может достигаться только через абсолютную, никем и ничем не ограниченную свободу. Приверженцев данной точки зрения едва ли беспокоят даже тривиальные вопросы: свобода для кого, свобода от чего, свобода быть или свобода иметь? Возможно, такие вопросы покажутся философскими и отвлеченными от практической дискуссии. Но, не разобравшись, чего же они хотят, сторонники либерального подхода тривиальным образом защищают не свободу и безопасность, а диктат, политическую и финансовую выгоду тех, кто на самом деле контролирует и использует интернет, облегчают жизнь распространителям детской порнографии и инструкций по проведению терактов, торговцам оружием и наиболее опасными товарами и услугами. Никому не хочется таскать каштаны из огня для других, но многие не понимают, что делают именно это.

Но уверены ли они, что Всемирная паутина сейчас действительно свободна, и хотят ли они именно такой свободы для нее в будущем? Интересно, как изменится их риторика в будущем, когда интернет разделится на несколько глобальных сетей. Будет ли входить в их понимание свободы свобода конкуренции новых

сетей друг с другом? Еще одной альтернативой будет фрагментация сети, предполагающая формирование множества зеркал отдельных доменов или их групп, теоретически локализованных в одной стране.

Подлинным жупелом для либералов является угроза контроля над контентом в социальных сетях, и убедить их в том, что подобный контроль не под силу ни одной структуре, даже целому государству, невозможно. Добиться полного контроля не удалось даже в отношении обычной почты, а уж тем более утопично такое предположение в отношении электронных средств, работающих в реальном времени вне географических границ. А в данном случае затрагиваются вопросы соотношения суверенитета, свободы и ответственности. Можно ли решить их в рамках такой концепции? Сомнительно…

Сторонники бумажной информации

Консерваторы, вероятно, решили навсегда заморозить свое сознание на уровне рубежа XIX в., ратуя за безопасный обмен информацией, обеспечение возможности ограничения доступа к документам. Представителей этой группы сегодня уже немного и становится все меньше. Однако, как ни странно, именно глубоко консервативное понимание *информации как документа* закрепляет основная масса правовых норм как в России, так и в других странах.

Консерваторы тоже не всегда знают, чего хотят. Никто не может определить, что такое документ — бумага с текстом или нечто иное? Что является его достаточным признаком — регистрационный номер или же текст? А что делать с чертежами и рисунками? И подобных вопросов масса: является ли документом один лишь номер; как определить, есть ли смысл в тексте или рисунке на документе; и, в итоге, что именно следует сохранять и чем обмениваться при работе с документом? Отсутствие полноценных ответов на эти вопросы подрывает основу взгляда на *информацию как документ*.

Прагматики

Прагматики учитывают все формы существования и перемещения информации и относят информацию к фундаментальным, имманентным бытию, категориям. Я отношу себя к этому течению. На этих позициях изначально стоят военные, относящие к информационным средствам радиоэлектронную борьбу, бомбы — выключатели электричества, химические и биологические средства, приводящие в негодность электронную аппаратуру, психотропные средства и многое другое. Определяющим выступает принцип воздействия на информацию, системы ее обработки, в том числе человеческое сознание, а также системы ее передачи и хранения.

Понятно, что такой подход предполагает существенно более широкое определение информации. Информация как таковая не связана непосредственно с человеком, ее следует рассматривать не только как смысловой результат деятельности мозга, порожденный и локализованный в нем, а как коммуникативную основу любого взаимодействия. Информацией обмениваются все объекты как материального, так и идеального мира, способные к взаимодействию; ее передача и получение возможны в разное время. Информация существует в компьютерных сетях и сетях связи, где человека нет физически и где он не участвует непосредственно в процессе ее передачи. Если учитывать эти утверждения, становится понятно, почему можно обеспечивать целостность и доступность информации в оптических линиях связи, где и электронных импульсов-то нет. Становится легче объяснить, что гены являются носителями информации, а также почему информация выполняет системообразующую функцию и является основой управления в любой сложной системе[6].

АЛОГИЗМЫ?

Три направления, рассмотренные выше, отличаются *подходами* к проблеме информационной безопасности и ставят во главу угла разные ее аспекты: три подхода и три поля борьбы за информационную безопасность и три видения ее задач.

Сторонники *первого подхода* стремятся закрепить или перераспределить права на управление интернетом и в то же время сохранить или перераспределить немалые финансовые потоки, связанные с обладанием этими правами. Именно поэтому основную роль здесь играет МСЭ, один из крупнейших игроков или, точнее, дилеров на этом рынке. Поэтому, не скрывая свой интерес, ему противостоят Соединенные Штаты, создавшие интернет, в значительной степени контролирующие его и не желающие расставаться со своими естественными на него правами. *Второй подход* представляет собой старое и, вероятно, отмирающее направление, которое, как на выборах, скорее отвлекает голоса от *оппозиции*, чем предлагает собственный путь. Под оппозицией, как читатель уже понял, понимаются сторонники *третьего, прагматического подхода*. Российская Федерация здесь играет значительную роль, но на ней список прагматиков не заканчивается. На Всемирном форуме по информационному обществу представители практически всех стран проголосовали за интернационализацию управления интернетом, причем выдвинула эту идею не Россия, а Евросоюз. Представителей ЕС не остановил даже прямой конфликт по этому поводу с присутствовавшей на форуме делегацией *большого брата*.

Однако проблему, по-видимому, следует определять иначе. Интернационализация управления интернетом, безусловно, представляет собой правильный и позитивный процесс, но проблема не в этом. Информационное (не только кибер-[7]) пространство не должно быть уязвимо само по себе и, одновременно, не должно являться источником или каналом реализации военных, террористических или криминальных (неразделимая триада) угроз для других сфер социальной активности человечества. И государство, пока оно является основным членом международного сообщества, должно быть гарантом информационной безопасности и отвечать за действия, совершаемые с его территории или из его информационного пространства. В первую очередь это касается угрозы активного противоборства (то есть военных действий) в информационной сфере. Именно государству общество делегировало функцию обеспечения безопасности, причем не только внешней, но и внутренней.

Противники введения в информационном пространстве каких бы то ни было правил, норм и других ограничений нередко апеллируют к правам человека, в частности к статье 19 Всеобщей декларации прав человека[8], гласящей: «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и *свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ* [здесь и далее курсив автора статьи. — *А. Ф.*]».

Однако при этом из аргументации «поборников прав человека в Сети» ускользает тот факт, что предпоследняя 29-я статья Декларации четко показывает, что свобода одного кончается там, где начинается свобода другого. В частности, статья включает следующие положения: «1. Каждый человек имеет обязанности перед обществом, в котором только и возможно свободное и полное развитие его личности. 2. При осуществлении своих прав и свобод каждый человек должен подвергаться только таким *ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе*. 3. *Осуществление этих прав и свобод ни в коем случае не должно противоречить целям и принципам Организации Объединенных Наций*»[9].

Но разве применение информационных средств, как и любых других, в целях войны не противоречит целям и принципам ООН? Или, к примеру, способствует ли укреплению в обществе морали и порядка использование интернета для целей терроризма или распространения детской порнографии? С учетом этого правильнее все-таки воспринимать свободу лучше как осознанную необходимость и именно на этом принципе строить безопасность, в том числе информационную.

И вот здесь появляются те самые алогизмы развития.

Алогизм первый: право информационной войны

Из дискурса об информационной безопасности ушла военная составляющая. По крайней мере, ее не видно: ее не оспаривают, но при этом по существу и не рассматривают. Принятие мер по предотвращению военно-политических угроз информационной безопасности подменяется дискуссиями по мерам доверия в сфере обучения, повышения компьютерного потенциала, сокращения цифрового разрыва и т. п. Вероятно, с начала 1990-х гг. появились более важные и актуальные проблемы. Необходимо поддерживать статус-кво в нынешней расстановке сил в сфере военных информационных разработок, снять с повестки дня вопросы о контроле над производством и принятием на вооружение информационных средств воздействия, интернационализации управления интернетом и завязанных на него потоках денег, сохранить возможность влияния через подконтрольную *всемирную паутину* на социальные группы, СМИ и массовое сознание, вести широкую пропаганду своих идей и ценностей. В случае чего, в кризисной ситуации интернет вместе с GPS можно и отключить. Или наоборот, как это было в Югославии, отключить все, кроме него, а по его каналам доводить до населения и международной общественности *правдивые данные* о враждебном государстве и его структурах и, ломая общественное сознание, уже в потенции исключить противоборство.

Из всех подходов к рассмотрению проблемы военной информационной угрозы выделяется обсуждение применимости международного гуманитарного права к конфликтам в информационном пространстве. Россия всегда придерживалась позиции, что существующее право применимо к информационным операциям, но требует доработки, поскольку формировалось в годы, когда информационные угрозы просто не рассматривались в юридическом ключе[10]. В выпущенном в 1999 г. и переизданном в 2000 г. документе Пентагона было, напротив, четко сказано, что «в настоящее время в международном праве не существует никаких ограничителей на проведение информационных операций»[11]. Осенью 2004 г. в Стокгольме на конференции НАТО[12] с приглашением российской делегации этот же тезис убедительно обосновывался европейскими военными юристами.

Но в 2009 г. в ходе работы второй ГПЭ МИБ правительственный эксперт США вдруг упомянул другой подход, выделив принципы *jus ad bellum*[13] и *jus in bello*[14] как вполне приемлемые для разрешения конфликтов в киберпространстве. После этого все сторонники названных принципов единодушно прозрели и поняли, что современное право вполне применимо к конфликтам в информационном пространстве. И ничего больше не надо, никаких дополнительных соглашений, конвенций, договоров, кодексов — все уже имеется: *jus ad bellum* и *jus in bello* в совокупности полностью покрывают данную проблематику. Остается лишь понять, в чем логика столь внезапного пересмотра подходов, и есть ли она вообще.

Алогизм второй: а о чем вообще речь?

На сегодняшний день информационная безопасность разделилась или, можно сказать, размножилась: появились информационная безопасность бизнеса, информационная безопасность культуры и т.д., однако сущностное наполнение этих концепций зачастую недостаточно и поверхностно, если вообще близко подходит к проблеме информационной безопасности — все чаще встречаются иссле-

дования по вопросам надежности автоматизированных систем вычислительных комплексов или практике журналистики и взаимодействия с общественностью, то есть *не о том*.

Все стремятся обеспечить информационную безопасность, но никто при этом не пытается понять, что такое информация, где она и как существует. Здесь комментировать нечего. Стоит лишь привести в качестве примера подход в целом очень серьезного и интересного издания *Новой философской энциклопедии*[15]. Статья *Информация* этого издания ограничивается отсылкой к статье *Информации теория*[16]. В свою очередь, отсылочная статья гласит, что указанная теория есть «специальная научная дисциплина… анализирующая математические аспекты процессов сбора, передачи, обработки и хранения информации»[17]. Об информации как таковой в ней более не сказано ни слова. Столь же интересна трактовка основного закона в этой области — закона об информации, информационных технологиях и защите информации. Здесь информация определяется как «сведения (сообщения, данные) независимо от формы их представления». При этом, что такое *сведения (сообщения, данные)* в законе не определяется, не говоря уже о том, что эти понятия относятся только к человеческому сознанию.

Аналогичная ситуация наблюдается и за рубежом. Электронный словарь Министерства обороны США, хотя и приводит термины *информационная безопасность, информационная атака, информационная операция* и др., термина *информация* не содержит. Попытка выйти из ситуации через переход к кибербезопасности делает ситуацию абсурдной: выходит, что мы боремся за свободу распространения и доступа к информации, сущность которой не понимаем, и защищаем технические средства и программы.

Алогизм третий: свобода мертвых душ

Как было сказано выше, наиболее многочисленная армия *борцов за информационную безопасность* выступает за свободу интернета, яростно отстаивая мысль о том, что глобальная сеть — это новый мир, который сформировал новую интернет-культуру. Но кто граждане этого мира? Передовая личность ассоциируется теперь с блогером, каждый уважающий себя человек, в том числе президент, имеет собственный блог, притом что еще пять лет назад в лучшем случае имел домашнюю страницу, а о блогах вообще никто не знал. Формируется представление, что весь мир завязан на интернет и блогосферу. Однако при серьезном обсуждении все специалисты в информационной безопасности в один голос говорят, что ни в одной из критических инфраструктур интернета нет — даже в серьезном бизнесе он кончается там, где кончаются отношения с клиентом. А интернет, по большому счету, — это только социальные сети.

Тогда какую же свободу столь бескомпромиссно защищают информационные либералы — свободу социальных сетей? И как много реальных интернет-пользователей? Как их подсчитывать? По IP-адресам, *никнеймам*? Или те, кто считает, имеют средства узнать, сколько у каждого человека адресов и имен в сети? А как, к примеру, считать тех активных пользователей, которых в период событий *Арабской весны* тысячами создавали специальные программы? Если признать их *мертвыми душами*, то следует отметить и то, что современные политические Чичиковы оказались гораздо более удачливы, чем герой Гоголя. Интернет–души не только продают и покупают, опираясь на их мнение и голоса, но и строят нужную международную политику, меняют неугодные режимы.

Алогизм четвертый: информация VS суверенитет

Информационная безопасность зачастую воспринимается как выражение антипода свободы распространения и доступа к информации.

Любое общество становится организованным лишь тогда, когда его члены начинают действовать в рамках выработанной им системы права. Основой общественной организации всегда являются нормы поведения и их сознательное выполнение. Однако в сфере международной информационной безопасности наблюдается, напротив, отрицание самой возможности введения норм и правил поведения государств и других субъектов отношений. Взамен предлагается *культура кибербезопасности*, а по сути — *альтруизма*.

В современном международно-политическом дискурсе по непонятным причинам противопоставляются идеи суверенитета государства над своим информационным пространством и ответственности государства за действия, совершенные из его информационного пространства. Общеизвестно, что обязанности могут основываться только на правах, и наоборот. Каким образом нести ответственность за что-то, над чем не имеешь прав суверенного контроля, в отсутствие которого ответственность также не может быть единоличной (а в нашем случае — *единогосударственной*)? Если установленный злоумышленник для интернет-атаки создал бот-сеть, размещенную на ресурсах десятка стран, должны ли эти страны также нести ответственность за его действия? Особенность метода создания бот-сетей заключается как раз в том, что владелец ресурсов не подозревает об их использовании злоумышленником. Чтобы отвечать за такого пользователя, государство, как минимум, должно располагать правом принуждения его к культуре кибербезопасности и использованию соответствующих средств контроля, которые могут быть помехой пользователю в его бизнесе, но он, тем не менее, будет обязан (по закону!) их исполнять.

Разве это — не одно из проявлений суверенитета? И наоборот, разве суверенитет не предполагает ответственность суверена за любые действия в тех сферах, на которые распространяются его суверенные права? Весьма уместно здесь было бы принятие кодекса поведения стран в информационном пространстве. Идея разработки такого кодекса присутствует и в разработанной администрацией США и презентованной Бараком Обамой 22 мая 2011 г. Международной стратегии по действиям в киберпространстве. Основой для кодекса вполне могли бы послужить предложенные четырьмя странами ШОС на 66-й сессии Генассамблеи ООН Правила поведения в области международной информационной безопасности[18]. Такой документ мог бы стать основой для внедрения на международном уровне культуры кибербезопасности, которая естественным образом проецировалась бы на национальный уровень. Однако и эта идея упорно отклоняется. Не совсем ясно, в чем заключается логика таких действий.

Алогизм пятый: противоречия в идеях теоретиков либерального лагеря

Либералы выступают категорически против отнесения социальной сферы к области информационной безопасности, однако при этом делают акцент на интернете и социальных сетях. Ни у кого не вызывает сомнений, что демократическое государство существует, для того чтобы обеспечивать государственную и общественную безопасность и, в частности надежную работу критических инфраструктур, — это его основные функции, именно эти права ему делегировало общество, и вопрос о суверенитете в данном случае никем не поднимается.

При этом появление таких убедительных свидетельств военного применения информационных технологий, как *Stuxnet*, *Duqu*, *Flame* и *Gauss*, не изменило акцентов дискуссии. Военные эксперты США и России включили появление *Stuxnet* в десятку самых серьезных военных событий 2010 г., причем отнюдь не в конце списка. В ответ прозвучали лишь разрозненные голоса, напомнившие, что в тех областях, где подобные *Stuxnet* средства могут нанести наибольший ущерб (управление технологическим процессом на крупных и особо опасных производствах, в энергетике, транспорте и пр.) обеспечить безопасность в настоящее время может только государство и только на основе суверенных прав. В данном случае такие фундаментальные права человека, как право на доступ к информа-

ции и право на распространение информации, за которые так радеют либералы, никак не ущемляются. Интересно, а как они мыслят его реализацию в системе, например, трансконтинентального нефтепровода или АЭС? Следуя такой логике, правила дорожного движения ущемляют фундаментальное право свободы передвижения и противоречат интересам развития, ограничивая мобильность рабочей силы. И если, к примеру, предложение передать функции обеспечения защиты от ракетно-ядерной угрозы от вооруженных сил обществу будет воспринято не иначе как признак серьезного заболевания, то почему в отношении информационной безопасности предлагается устранить государство и руководствоваться лозунгом «спасение утопающих — дело рук самих утопающих»?

Можно продолжать и далее, но и без того очевидно, что построение логичной и адекватной концепции информационной безопасности для использования в международных и общественных отношениях еще далеко до завершения.

***

Уже почти 15 лет Россия и мировое научное сообщество[19] прилагают значительные усилия к тому, чтобы предотвратить превращение информационного пространства, ставшего одной из ключевых критических инфраструктур человечества, в поле боя. В целом эту же цель поставила перед собой и ООН. Однако — и это тоже следует признать — ее достижение пока не просматривается.

Главный вопрос информационной безопасности, наверное, можно было сформулировать как классическую философскую антитезу бытия: «Человек с оружием или человек с орудием». Было бы правильно, если бы идея международной информационной безопасности стала основой философии мира в постмодерне, а не постиндустриальным вариантом идеи противостояния войне. Но пока, к сожалению, информационная безопасность в общественном дискурсе выглядит некоей совокупностью бодрияровских симулякров, которые вытесняют и подменяют собой собственные смыслы рассматриваемых проблем.

Александр Федоров,
член Экспертно-консультативного совета ПИР-Центра
fedorov-av@bk.ru

Примечания

[1] Источник цитаты умышленно не приводится, дабы не ставить специалистов данной страны в неудобное положение, однако речь идет о документе 2012 г., который имеется в распоряжении автора; в тексте дается точное цитирование.

[2] Соглашение между правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. (Екатеринбург. 16.06.2009.) Текст имеется в распоряжении ПИР-Центра.

[3] Этот термин также продолжает существовать и не только в российской терминологии. Современный электронный словарь военных терминов Министерства обороны США (http://www.dtic.mil/doctrine/dod_dictionary/, последнее посещение — 3 сентября 2012 г.) дает не совпадающую с российской, но вполне приемлемую дефиницию этого термина: *информационная безопасность* — защита информации и информационных систем от несанкционированного доступа или модификации информации при ее хранении, обработке или транзите от отказа в обслуживании зарегистрированным пользователям. (Источником указан документ, приведенный в следующей сноске).

[4] Joint doctrine for information operations, JCS, Joint Pub 3–13, 8 October 1998.

[5] Надо полагать, из Вашингтона мониторинг военных угроз вести сподручнее. Если верить еженедельнику Jane's Defense Weekly (цитируется по «Пентагон принимает «План X». *Красная Звезда.* 2012, 25 августа. № 155) только по линии DARPA [Агентство передовых обо-

ронных исследовательских проектов] на разработки в области кибертехнологий Пентагону в 2012 г. выделено 208 млн долл.

[6] См. подробнее: Расторгуев С. П. Философия информационной войны. М.: Психолого-социальный институт, 2003.

[7] Если следовать американской официальной логике, киберпространство представляет собой систему открытых сетей связи и подключенных к ним компьютеров с соответствующим программным обеспечением, то есть *интернет без информации и пользователей*. Кибербезопасность включает безопасность сетей связи, компьютеров и программного обеспечения для их функционирования. Информационное пространство понимается как совокупность всех сфер применения информационно-телекоммуникационных средств и технологий (ИКТ), обрабатываемая в них информация и люди, занятые в этой среде. Словарь военных терминов Министерства обороны США определяет киберпространство как «глобальную область в пределах информационной окружающей среды, состоящей из взаимосвязанной сети информационных инфраструктур и технологии, включая Интернет, телекоммуникационные сети, компьютерные системы, и вложенные процессоры и диспетчеров». Примечательно, что термин *кибербезопасность* словарь Минобороны США не содержит. Соответственно, понимание информационной безопасности даже в американской военной трактовке оказывается существенно более широким и содержательно наполненным и действительно может рассматриваться как безопасность информационного общества, где все основные сферы деятельности самым непосредственным образом основаны на ИКТ.

[8] Всеобщая декларация прав человека. Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 г. Декларации. Организация Объединенных Наций, http://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (последнее посещение — 9 октября 2012 г.).

[9] Там же, Статья 29.

[10] Одним из первых экспертных центров, выдвинувших такой подход, был ПИР-Центр, который в 2001 г. опубликовал следующую монографию, содержавшую соответствующие разделы:

И. Ю. Алексеева и др. Информационные вызовы национальной и международной безопасности. Под общ. редакцией А. В. Федорова и В. Н. Цыгичко — М.: ПИР-Центр, 2001.

[11] An Assessment of International Legal Issues in Information Operations, DOD, March 1999.

[12] International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17–19 November 2004.

[13] Право объявлять войну как часть международного права в области прав человека.

[14] Право войны или право вооруженных конфликтов.

[15] Новая философская энциклопедия в 4-х томах. М.: Мысль, 2001.

[16] Там же. С. 143.

[17] Там же. С. 141.

[18] Документ 66-й сессии Генеральной ассамблеи ООН А/66/359, распространен 14 сентября 2011 г.

[19] В 1999 г. Всемирная конфедерация ученых на ежегодной конференции в Эриче (Италия) признала, что в XXI в. основные угрозы человечеству будут носить информационный характер.