ЖЕНЕВСКИЙ ЦЕНТР ДЕМОКРАТИЧЕСКОГО
КОНТРОЛЯ НАД ВООРУЖЕННЫМИ СИЛАМИ (DCAF)

ДЕМОКРАТИЧЕСКОЕ УПРАВЛЕНИЕ И ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ

Бенджамин С. Бакленд, Фред Шрайер,
Теодор Х. Винклер

Женевский центр демократического контроля над вооруженными силами (DCAF)

DCAF HORIZON 2015 WORKING PAPER No. 1.RU

ДЕМОКРАТИЧЕСКОЕ УПРАВЛЕНИЕ И ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ

Бенджамин С. Бакленд, Фред Шрайер, Теодор Х. Винклер

ЖЕНЕВА – 2013

Бенджамин С. Бакленд, Фред Шрайер, Теодор Х. Винклер, *Демократическое управление и вызовы кибербезопасности* (Женева: Женевский центр демократического контроля над вооруженными силами, 2013).

DCAF Horizon 2015 Working Paper No. 1.RU

Оригинальное издание на английском языке, 2009
Русская версия, 2013
Исполнительный издатель: ООО Прокон, http://procon.bg
Дизайн обложки: Ангел Недельчев
ISBN 978-92-9222-223-9

ДЕМОКРАТИЧЕСКОЕ УПРАВЛЕНИЕ И ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ

Бенджамин С. Бакленд, Фред Шрайер, Теодор Х. Винклер

Женева – 2013

Женевский центр демократического контроля над вооруженными силами (ДКВС)

www.dcaf.ch

Женевский центр демократического контроля над вооруженными силами является одним из ведущих учреждений в мире в сфере реформирования сектора безопасности (SSR) и управления сектором безопасности (SSG).

Женевский центр демократического контроля над вооруженными силами (ДКВС) оказывает консультативную поддержку на местах, организовывает программы практической помощи, разрабатывает демократические нормы по соответствующим вопросам и продвигает их как на международном уровне, так и на уровне отдельных государств, а также пропагандирует передовой опыт и создает политические рекомендации по вопросам обеспечения эффективного демократического управления в сфере безопасности.

Центр ДКВС сотрудничает с правительствами государств, парламентами, гражданским обществом, международными организациями, а также целым рядом структур безопасности, в частности, органами полиции, судебной власти и разведки, пограничными службами и вооруженными силами.

Оглавление

О чем эта книга ..... **vii**

Вступление **1**

1. Кибер-угрозы, их источники и субъекты борьбы с ними **4**

1.1. Кибер-угрозы 4

1.2. Субъекты борьбы с кибер-угрозами 4

2. Проблемы демократического управления **13**

2.1. Надзор 13

2.2. Борьба с кибер-угрозами в контексте соблюдения гражданских прав и свобод 17

2.3. Средства сдерживания и противодействия в кибер-войне 23

Выводы **30**

Список использованной литературы **33**

Приложение 1: Защита критической инфраструктуры, защита критической информационной инфраструктуры и кибербезопасность **35**

Приложение 2: Меры противодействия международного и регионального уровней **47**

О чем эта книга

Проблемы обеспечения безопасности в киберпространстве не имеют границ. Однако каждое государство решает их в основном самостоятельно, поэтому даже всех предпринятых мер оказывается недостаточно. Существуют огромные пробелы как в нашем понимании проблемы кибербезопасности, так и в государственной политике и технических возможностях, необходимых для ее решения. Кроме того, при обсуждении этой проблемы почти полностью упускаются из виду вопросы демократического управления, особенно в сфере контроля, надзора и прозрачности. Эти вопросы значительно усложняются ввиду присутствия в секторе компьютерной безопасности огромного количества частных игроков, действующих как самостоятельно, так и в сотрудничестве с органами государственной власти. Учитывая темп, набранный государствами и частными компаниями в сфере укрепления безопасности компьютерных сетей и подготовки к войне в киберпространстве, сегодня как никогда остро встают вопросы, связанные с несовершенством системы демократического управления. Именно этим вопросам мы и уделили основное внимание в нашей публикации.

Вступление

Для термина «киберпространство» существует множество определений, каждое из которых дает собственное толкование этого понятия. В данной публикации мы рассматриваем киберпространство как *комплекс взаимосвязанных между собой информационно-технологических инфраструктур*. Сюда входят всемирная компьютерная сеть Интернет, телекоммуникационные сети, компьютерные системы, а также встраиваемые процессоры и контроллеры, использующиеся в различных отраслях промышленности.[1]

За последних два десятилетия мы стали свидетелями информационного «взрыва», когда практически ни один человек уже не может обойтись без доступа к информационным сетям. Повсеместное распространение глобальной сети Интернет требует повышенного внимания к вопросам взаимосовместимости сетей, эффективности и свободы доступа к информации. Вместе с тем, рост интереса к глобальной сети не сопровождается адекватными мерами по обеспечению ее безопасности. Это является следствием того факта, что изначально Интернет создавался для обмена научными данными, а не для поддержки всей мировой экономики, как это происходит сегодня. Стремительный рост масштабов использования и функционирования всемирной компьютерной сети Интернет (как в конструктивных целях, так и деструктивных) опережает усилия по реформированию и обеспечению безопасности его первоначальной инфраструктуры.[2]

Кибербезопасность или безопасность всемирной сети Интернет (что по сути одно и то же) предполагает решение задач в глобальном масштабе, в то время как подавляющее большинство мер противодействия осуществляются на уровне отдельных государств, и их явно недостаточно. Существуют огромные пробелы как в нашем понимании проблемы кибербезопасности, так и в государственной политике и технических возможностях, необходимых для ее решения. Кроме того, при обсуждении этой проблемы практически полностью упускаются из виду вопросы демократического управления, особенно в сфере контроля, надзора и прозрачности. Эти вопросы значительно усложняются ввиду присутствия в секторе компьютерной безопасности огромного количества частных игроков, действующих как самостоятельно, так и в сотрудничестве с органами государственной власти. Учитывая темп, набранный государствами и частными компаниями в сфере укрепления безопасности компьютерных сетей и подготовки к войне в киберпространстве, сегодня как никогда остро встают вопросы, связанные с несовершенством системы демократического управления. Именно этим вопросам мы и уделили основное внимание в нашей публикации.

---

[1] Авторы благодарят Тобиаса Боллигера, Белинду Клиленд, Аню Эбнотер, Пола Мейера, Даниэля Стауффахера, Барбару Викс и Айдана Уилса за их полезные и актуальные замечания по содержанию материала. Также ДКВС хотел бы выразить особую признательность Женевскому Форуму по вопросам безопасности (Geneva Security Forum) за сотрудничество и содействие в подготовке данной публикации.

[2] Lloyd's Emerging Risks Team, *Digital Risks: Views of a Changing Risk Landscape* (London: Lloyds, 2009).

Как видно из представленного ниже материала, существует огромное разнообразие как самих кибер-угроз, так и субъектов борьбы с ними. Однако если рассматривать эту проблему с точки зрения прозрачности, контроля и надзора, все эти угрозы можно условно разделить на две большие группы.

Правительства государств, конечно же, в первую очередь волнуют вопросы национальной безопасности и защиты критической информации и своих информационных инфраструктур от посягательств как государственных, так и негосударственных субъектов или группировок, которые могут их похитить, передать, уничтожить или иным способом нарушить их целостность. Реальную угрозу для безопасности государства представляют кибер-атаки, направленные на вывод из строя его систем телекоммуникации, энергогенерирующих и нефтеперерабатывающих мощностей, системы электроснабжения, финансовой системы, а также системы здравоохранения и других жизненно важных инфраструктур.[3] Пример Эстонии (см. вставку 3) показывает, что такие опасения вовсе не беспочвенны, а многие факты свидетельствуют о том, что война в киберпространстве – а именно так можно в целом охарактеризовать этот новый тип угрозы – кардинально изменит характер современной войны, точно так же, как он периодически менялся под влиянием научно-технического прогресса в прошлые десятилетия.[4] Можно с уверенностью утверждать, что кибервойна откроет новую главу в истории военного дела и займет место кинетической энергии как главного средства поражения противника. Участие в кибервойне требует ответов на такие вопросы, как а) что следует относить к объектам жизненно важной инфраструктуры, б) по каким признакам то или иное действие следует квалифицировать как нападение и в) какую роль может или должен играть сектор безопасности в обеспечении обороны или осуществлении ответной атаки. Как мы увидим далее, кибервойна стирает различия между военными и гражданскими объектами атаки, как и различия между теми, кто эти атаки осуществляет. Это, в свою очередь, ставит на повестку дня такой важный вопрос, как определение надежных и в то же время законных мер противодействия, которые государство может предпринять в случае начала масштабной кибервойны. То есть следует определиться, в каких случаях это должен быть дипломатический демарш, официальный протест или введение экономических санкций, а в каких привлечение к уголовной ответственности или военный удар.[5]

Еще важнее ответить на вопрос о том, какие процессы демократического управления и какие юридические нормы должны определять решения о применении тех или иных ответных мер. Последний пункт имеет особое значение, учитывая, что существует целый ряд факторов, которые существенно снижают прозрачность кибервойны по сравнению с другими типам конфликтов. Эти факторы будут рассмотрены более подробно в заключительной части данного исследования. Однако о некоторых из них следует сказать в самом начале. Во-

---

3 White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington DC: White House, 2009).

4 John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Washington DC: RAND, 1997).

5 John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, 25 января 2010 г., World section.

первых, кибератака, в отличие от обычного вооруженного нападения, проходит бесшумно, т.е. без взрывов и грохота канонад. Для обнаружения, определения типа атаки и принятия решения о мерах противодействия требуются технические и узкоспециализированные знания, в частности те, которые используют для защиты своих сетей структуры частного сектора. Это сильно снижает уровень прозрачности при осуществлении масштабных кибератак или контратак. Они могут произойти и без вмешательства надзорного органа (например, соответствующего парламентского комитета), который может вообще не узнать о факте нападения. Кроме того, из-за сугубо технического характера проблемы, в данном случае значительно возрастает роль разведслужб (по сравнению с правоохранительными структурами), что еще больше снижает уровень прозрачности а, соответственно, и возможности для осуществления контроля и надзора.

Угрозу для национальной безопасности и государственных объектов критической инфраструктуры (в широком смысле) могут пока представлять только некоторые из видов атак, существующих сегодня в арсенале кибер-диверсантов. Более серьезной проблемой, которой и посвящено данное исследование, является вопрос о том, как обеспечить демократический контроль в сфере регулирования деятельности в Интернете и использования информационной инфраструктуры с целью пресечения деструктивных действий отдельных лиц и других субъектов кибер-преступности. Таким образом, в данном случае речь идет не столько о самой войне в информационном пространстве или уязвимости национальной инфраструктуры к кибер-атакам, сколько о таких явлениях, как цензура, несанкционированный контроль электронной переписки или деятельность интернет-провайдеров по сбору и хранению персональных данных (часто по требованию властей и в сотрудничестве с ними).

Поэтому проблемы безопасности в кибер-пространстве обсуждаются в контексте общих вопросов безопасности, когда речь заходит о противоречиях между интересами национальной безопасности и безопасности человека. Именно соблюдение оптимального баланса между интересами государственной безопасности и человеческой безопасности и составляет главную проблему борьбы с преступностью в кибернетическом пространстве. К этому уравнению нужно добавить еще и третий важный компонент, который условно можно назвать «безопасностью частной собственности», что в данном случае подразумевает безопасность корпораций и частных компаний.

Борьба с киберпреступностью предполагает решение трех задач. Первые две задачи иногда взаимосвязаны между собой и заключаются в укреплении безопасности общества и частной собственности путем защиты компьютерных сетей от внешних вторжений, с одной стороны, и нейтрализации криминальных и экстремистских группировок, использующих эти сети в своих преступных целях, с другой стороны. Это те задачи, при решении которых не обойтись без создания комплексных механизмов государственно-частного партнерства. Другой не менее важный аспект борьбы с киберпреступностью состоит в том, что используемые при этом меры противодействия могут противоречить принципам демократического управления. Поэтому очень важно, чтобы деятельность субъектов публичного и частного секторов по защите компьютерных сетей и отслеживанию проходящих по ним информационных потоков

максимально учитывала принципы человеческой безопасности, в частности, в отношении таких основополагающих прав человека, как право на неприкосновенность частной жизни, право на свободу выражения своих убеждений и право на свободу объединений.

Учитывая проблематику данного исследования, дальнейший материал мы разделили на две больших части. В первой представлен краткий обзор основных кибер-угроз и субъектов борьбы с ними, особенно в контексте государственно-частного партнерства. Вторая часть посвящена ключевым вопросам демократического управления. Она состоит из глав, рассматривающих вопросы контроля и надзора, защиты прав человека и, наконец, проблемы демократического управления, которые могут возникнуть в контексте борьбы с киберпреступностью.

1. Кибер-угрозы, их источники и субъекты борьбы с ними

1.1. Кибер-угрозы

Одна из главных проблем борьбы с киберпреступностью заключается в том, что часто бывает чрезвычайно трудно точно установить не только самих исполнителей преступления, но даже страну их пребывания. Поэтому преступник или преступная группа могут относительно легко скрыть свое участие в кибер-атаке либо выдать себя за другого пользователя сети.[6] Более подробно этот вопрос будет рассмотрен ниже. В двух следующих таблицах приводятся краткие описания основных участников киберпреступности (пока без учета проблемы их идентификации) и решаемых ими задач.

1.2. Субъекты борьбы с кибер-угрозами

Одна из главных проблем борьбы с кибер-угрозами (и один из вопросов, которым посвящен проект «Горизонт 2015»/Horizon 2015 Project) состоит в том, что большинство информационно-коммуникационных сетей принадлежат субъектам частного сектора, в то время как часть общей *ответственности* за их безопасность, как правило, лежит на государстве.[7] К этому вопросу мы еще вернемся, а сейчас хотелось бы отметить, что участие в этом процессе частных субъектов значительно усложняет задачу обеспечения безопасности киберпространства в контексте соблюдения принципов демократического управления. Эти две группы субъектов, то есть государство с одной стороны и частные игроки с другой, преследуют разные интересы. Это снижает эффективность усилий по защите информационного пространства и в то же время не позволяет при этом обеспечить необходимый уровень защиты фундаментальных прав и свобод человека.

Эти трудности усугубляются еще больше ввиду глобального характера как самой проблемы, так и способов ее решения. В данном случае определенную роль в разработке международных норм в соответствующей сфере и опреде-

---

6 Markoff, Sanger, and Shanker, “In Digital Combat, U.S. Finds No Easy Deterrent.”

7 Jennifer Wood and Benoît Dupont, eds., *Democracy, Society and the Governance of Security* (Cambridge: Cambridge University Press, 2006).

лении наиболее эффективных методов противодействия могли бы сыграть международные субъекты борьбы с киберпреступностью. Международные субъекты могли бы выступить в роли катализаторов процессов, направленных на гармонизацию национальных законодательств, регулирующих вопросы ведения следствия, привлечения к уголовной ответственности, обеспечения сохранности данных и защиты неприкосновенности частной жизни, а также принципы обеспечения сетевой безопасности и оперативного реагирования на атаки. Кроме того, они могли бы помочь в выявлении слабых мест в системе надзора и в выработке эффективных методов демократического контроля над деятельностью субъектов и государственно-частных партнерств в сфере борьбы с киберпреступностью. Этому вопросу следует уделить особое внимание, учитывая, что предпринимаемые международными игроками усилия по выработке комплекса эффективных методов противодействия (в частности, речь идет о Подгруппе Большой Восьмерки по вопросам высокотехнологичной (или кибер-) преступности, Конгрессе ООН по вопросам профилактики преступности и уголовного правосудия и Конференции Совета Европы по вопросам сотрудничества в сфере борьбы с киберпреступностью) по большей части сосредоточены на вопросах эффективности, но не прозрачности и контроля, о чем мы поговорим чуть далее.

Значение прозрачности, контроля и надзора возрастает еще больше ввиду огромных различий в технических возможностях и законодательствах разных государств. Одни страны, в частности США и Великобритания, вкладывают огромные средства в программы борьбы с киберпреступностью и модернизации соответствующей нормативно-правовой базы, в то время как другие не имеют даже самой базовой информационной инфраструктуры, не говоря уже о стратегиях борьбы с кибер-угрозами, как направленных против них самих, так и исходящих с их собственной территории. Поэтому необходимо разработать законодательство, которое бы регулировало сферу кибербезопасности (в том числе и вопросы эффективного демократического контроля) и борьбы с киберпреступностью. Если отсутствие технических возможностей для борьбы с киберпреступностью усугубляется еще и отсутствием соответствующей нормативно-правовой базы, проблема раскрытия подобных преступлений и привлечения их исполнителей к ответственности становится практически неразрешимой. А отсутствие в стране специально уполномоченных надзорных органов увеличивает риск того, что в ней будут нарушаться права человека на свободу выражения мнений, неприкосновенность частной жизни и свободу объединений.

Для борьбы с киберпреступностью на международном уровне приняты такие правовые акты, как Резолюции Генеральной Ассамблеи ООН № 55/63 от 4 декабря 2000 года и № 56/121 от 19 декабря 2001 «Борьба с использованием информационных технологий в преступных целях», а также «Основные принципы совместной работы правоохранительных органов и интернет-провайдеров в сфере борьбы с киберпреступностью», принятые на Всемирной конференции «Сотрудничество против киберпреступности» (Страсбург, 1–2 апреля 2008 года). Среди правовых актов регионального уровня следует упомянуть Рекомендацию Совета Европы № R(89)9 «О борьбе с компьютерными преступлениями» и Европейскую Конвенцию «О борьбе с киберпреступностью». Согласно этой конвенции, государства-члены Совета Европы должны законода-

тельно утвердить полномочия и процедуры для проведения расследований, а также для сбора электронных доказательств в отношении уголовных преступлений, совершаемых с использованием компьютерных технологий. Непосредственное отношение к борьбе с киберпреступностью имеют и некоторые документы международного и регионального права, касающиеся защиты прав человека. Это *Международный пакт о гражданских и политических правах* (в частности, Статья 17 о праве на неприкосновенность частной жизни, Статья 19 о праве на свободу выражения мнений и Статья 22 о праве на свободу объединений), *Европейская конвенция по правам человека*, *Африканская хартия прав человека и народов*, а также *Американская конвенция по правам человека*.

Помимо этих вопросов, международные и региональные организации предпринимают меры и для защиты электронных данных. Так, например, Генеральная ассамблея ООН утвердила «Принципы регулирования компьютеризированных баз персональных данных», а Совет Европы принял Конвенцию «О защите физических лиц при автоматизированной обработке персональных данных». Оба эти документа содержат положения, направленные на защиту прав человека на неприкосновенность частной жизни и свободу выражения мнения при ведении электронной переписки и размещении персональных данных в компьютерных сетях.

Еще одним ключевым субъектом борьбы с киберпреступностью являются рядовые пользователи сетей. Поэтому очень важно вовлекать их в просветительские мероприятия, которые помогут им лучше разбираться в таких вопросах, как компьютерное мошенничество, хищение личных реквизитов, преступления в интернете, этика интернета, а также связанные с этим права пользователей всемирной сети.

В таблице 3 перечислены некоторые из основных субъектов, участвующих в противодействии кибер-угрозам.

Таблица 1. Источники кибер-угроз [8]

Источник угрозы	Описание угрозы
Государство	Разведслужбы иностранных государств используют компьютерные технологии для сбора информации и шпионажа. Подобные действия могут быть направлены против других государств (как дружественных, так и враждебных) или против негосударственных субъектов кибератак. Государства могут осуществлять кибератаки против недружественных государств с целью дезинформации, дестабилизации, устрашения или даже в рамках полномасштабной кибервойны. В нарушение принципов безопасности человека государственные органы могут также прибегать к таким средствам, как перехват и использование персональных данных, причем в некоторых случаях это происходит без соответствующей санкции судебных органов и без надлежащего демократического контроля.
Корпорации	Предприятия и корпорации (иногда при содействии организованных преступных группировок или хакеров) занимаются промышленным шпионажем и/или диверсиями. Как и в предыдущем случае, корпорации могут нарушать права человека путем сбора и анализа больших объемов персональных данных, а в некоторых случаях и путем обмена этими данными с государственными органами и другими частными субъектами.
Хакеры	Когда-то хакеры чаще всего занимались взламыванием сетей просто из хулиганских побуждений или для того, чтобы завоевать авторитет в хакерском сообществе, но сегодня их толкают на это другие причины, которые гораздо чаще имеет криминальный характер. Если раньше для взлома удаленных сетей требовались серьезные навыки и знание компьютерных технологий, то теперь хакеру достаточно скачать из интернета соответствующие инструкции и протоколы и использовать их для организации кибер-атак на выбранные им сайты. Таким образом, средства для осуществления кибер-атак стали более изощренными и доступными для использования.
Хактивисты	Термин «хактивизм» (hacktivism) возник из соединения двух слов “Hack” и “Activism.” Он обозначает новое явление социального протеста, которое представляет собой своеобразный синтез социальной активности, преследующей цель протеста против чего-либо, и хакерства, направленного против определенных веб-сайтов или почтовых серверов. Хактивисты стремятся повредить, исказить содержание или вывести из строя некоторые веб-сайты для достижения своих политических целей.

[8] По материалам United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, “Reflections on Cybersecurity,” *Science* 326 (13 November 2009): 943-4; См. Martin Charles Golumbic, *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (New York: Springer, 2007).

Кибер-диверсанты из числа недовольных пользователей сети	Недовольные пользователи представляют серьезную угрозу, учитывая, что они, как правило, хорошо знакомы с принципами работы системы и могут использовать свои знания в деструктивных целях, например, для повреждения системы или хищения конфиденциальных данных. По данным Федерального бюро расследований (ФБР) США, вероятность организации кибер-атак со стороны пользователей системы и внешних источников составляет 2:1.
Террористы	Своими действиями террористы стремятся уничтожить, вывести из строя или использовать в своих целях важнейшие объекты инфраструктуры, поставить под угрозу национальную безопасность, повлечь массовые человеческие жертвы, ослабить экономику, а также подорвать моральное состояние общества и его доверие к властям. Далеко не все террористические группировки пока обладают достаточными знаниями и техническими возможностями для осуществления эффективных кибер-атак, но теоретически они вполне могут получить такие знания и возможности (или даже прибегнуть к услугам организованных преступных группировок).
Ботнет	Бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Эти хакеры заражают своими программами большое количество компьютеров, которые они затем используют для координации атак, рассылки спама, перебора паролей на удалённых системах, фишинга и других вредоносных действий. Услуги таких сетей являются объектом нелегальной торговли.
Фишеры	Фишеры – частные лица или небольшие группировки, которые используют технологию фишинга (phishing – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям) с целью кражи персональных реквизитов или перепродажи ценной информации. Для достижения своих целей фишеры часто используют спамы и шпионские/вредоносные программы.
Спамеры	Спамеры – физические лица или организации, которые рассылают незатребованную электронную почту (часто со скрытой или ложной информацией) с целью рекламирования и продажи товаров, фишинга, распространения шпионского/ вредоносного ПО или осуществления кибер-атак на конкретные организации.
Создатели шпионского или вредоносного ПО	Физические или юридические лица с преступными намерениями, осуществляющие кибер-атаки на компьютеры пользователей посредством производства и распространения шпионского и вредоносного ПО.
Педофилы	Педофилы все чаще используют Интернет для обмена детской порнографией (посредством электронной почты, специализированных файлообменных сервисов и пирингового ПО), а также для знакомства с потенциальными жертвами (часто в социальных сетях или интернет-чатах).

Таблица 2. Виды кибер-угроз

Вид	Подвид	Примеры
Целостность данных При осуществлении кибер-атак могут использоваться хакерские методики с целью искажения или уничтожения данных либо нарушения их целостности иным способом.	Пропаганда/ дезинформация	Изменение или подтасовка данных либо введение недостоверных данных с целью оказания влияния на результаты политических процессов или коммерческой деятельности либо с целью дестабилизации правящих режимов на территории иностранных государств.
	Устрашение	Атаки на веб-сайты осуществляются для того, чтобы вынудить их владельцев (как государственных, так и частных) удалить или изменить их содержание либо изменить политику сайта.
	Уничтожение	Целенаправленное и постоянное уничтожение данных с целью нанесения вреда конкурентам либо иностранным государствам. В частности, такие атаки могут осуществляться наряду с другими действиями в рамках более масштабного конфликта.
Доступ Атаки на отказ в обслуживании, например с использованием ботнетов, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднен.	Внешняя информация	Атаки на отказ в обслуживании и другие виды атак на государственные и частные сервисы открытого доступа, в частности сайты СМИ и информационные сайты органов государственной власти и т.д.
	Внутренняя информация	Атаки на локальные сети частных или государственных служб, например, аварийно-спасательных служб, инфраструктуры управления энергетической и транспортной системами, сайты электронного банкинга, корпоративные сервисы электронной почты, системы оперативного управления и т.д.

Конфиденциальность Кибератаки могут быть нацелены на различные источники конфиденциальной информации и часто осуществляются в преступных целях.	Шпионаж	Поиск фирмами информации о своих конкурентах; участие государств в шпионской деятельности (направленной против иностранных государств и физических лиц).
	Хищение персональных данных	Фишинг или аналогичные виды атак, цель которых состоит в том, чтобы обманным путем вынудить пользователей сообщить свои персональные данные, например, номера банковских счетов; рассылка вирусов, которые копируют и загружают такие данные с компьютера пользователя.
	«Кража личности» (хищение персональных реквизитов)	Трояны и подобные им программы используются для кражи личных данных, которые затем используются при совершении преступлений.
	Поиск информации во всемирной сети	Для получения различной информации, в частности персональных данных, используется технология поиска информации из открытых источников.
	Мошенничество	Часто осуществляется через спам, который распространяется по электронной почте; самый известный вид подобного мошенничества – так называемые «нигерийские письма 419». Сюда же относятся мошеннические схемы с предложениями о предоплате услуг, которые никто не собирается оказывать, а также просьбы о предоплате несуществующих товаров.

Таблица 3. Субъекты противодействия кибер-угрозам

Категория	**Примеры**	**Роль**		
		Политика	***Ответная реакция***	***Надзор за соблюдением норм и правил***
Международные и региональные организации	Рабочая группа по телекоммуникациям и информации Азиатско-Тихоокеанского экономического сотрудничества (АТЭС/APEC-TEL), Европейское агентство сетевой и информационной безопасности (ЕСИАБ/ENISA), Объединенный центр передовых методов кибернетической обороны НАТО (ОЦПМКО/CCDCOE), Ассоциация стран Юго-Восточной Азии (АСЕАН/ASEAN), Организация экономического сотрудничества и развития (ОЭСР/OECD), Группа оперативного реагирования на чрезвычайные ситуации в компьютерных сетях OAS (КГРЧС/CSIRT), Форум по управлению Интернетом (ФУИ/IGF), Международный союз электросвязи (МСЭ/ITU), Общество Интернета (ОИ/ISOC), Интернет-корпорация по присвоению имен и номеров (ICANN), Гражданская инициатива Интернет-политики «Меридиан» (ГИИП/CIIP Meridian), Лионская группа Большой восьмерки, Подгруппа по преступности в сфере высоких технологий, ООН, Совет Европы	X	X (ICANN, ГИИП «Меридиан»)	X (Лионская группа Большой восьмерки, Подгруппа по преступности в сфере высоких технологий)
Неправительственные организации	Правозащитные организации (в частности, Американский союз защиты гражданских свобод, Международная правозащитная организация Human Rights Watch, «Международная амнистия» (МА/IA), «Репортеры без границ» (РБГ/RWB), Инициатива OpenNet), а также различные фонды (в частности, Фонд «World Wide Web», Фонд «Shadowserver»), аналитические центры (например, Центр стратегических и международных исследований (ЦСМИ/CSIS), Американский центр стратегических исследований RAND и многие другие)	X		

Отраслевые организации	Антифишинговая рабочая группа (APWG), Исследовательско-аналитический центр по вопросам функционирования службы доменных имен (ИАЦСДИ/DNS-OARC), Рабочая группа по борьбе со злоупотреблениями в системах передачи сообщений (MAAWG), Отраслевой консорциум по укреплению безопасности в Интернете (ICASI), Научно-технический совет по вопросам защиты информации и научно-исследовательская группа по вредоносным кодам при Научном совете по вопросам информационной безопасности (ISTSG), Международная комиссия по стандартам Интернета (ИСИ/IETF), Институт инженеров по электротехнике и электронике (IEEE), организации в сфере транспорта (в частности, обеспечивающие безопасность аэропортов и управление воздушным движением), другие отраслевые организации, связанные с управлением критической инфраструктурой	X (APWG)	X	
Государства	Министерства внутренних дел, иностранных дел, транспорта и финансов, разведывательные службы, управления полиции (в частности, специализированные подразделения по кибербезопасности и организованной преступности), министерства юстиции, Компьютерные группы экстренной готовности (КГЭГ/CERT), управления оперативной безопасности, специализированные управления по вопросам кибербезопасности	X	X	X
Частный сектор	Специализированные компании по обеспечению безопасности в интернете, разработчики программного обеспечения, производители оборудования, системы банковских электронных платежей, серверы электронной почты, хостинг-провайдеры, участники финансово-банковского сектора, компании, занимающиеся продажей товаров в интернете		X	
Физические лица	Физические лица – владельцы и пользователи ПК	X	X	

2. Проблемы демократического управления

2.1. Надзор

Государства, сталкивающиеся с угрозами национальной безопасности, как традиционными, так и нетрадиционными, не способны эффективно справиться с ними без помощи других участников. Эта проблема все чаще решается за счет создания децентрализованных систем управления безопасностью, в частности, через механизмы государственно-частного партнерства. На первый взгляд этот процесс напоминает «приватизацию» государственных функций. Однако, по мнению Элисон Бэйлс, такая трактовка не учитывает целого ряда нюансов и сложностей ситуаций, при которых в каждом конкретном случае принимается решение о полной либо частичной передаче определенных функций без «полной передачи права собственности [...], что произошло бы в случае приватизации промышленных объектов».[9]

Когда мы говорим о проблеме кибербезопасности, то в данном случае более уместно было бы использовать термин «*система управления*», учитывая, что *делегирование либо передача ответственности* происходят одновременно по двум направлениям. Государства могут действовать на уровне частных компаний, и точно так же частные компании могут действовать на уровне государства. В качестве примера можно привести соглашение о сотрудничестве, подписанное недавно между компанией Google и Агентством Национальной безопасности США (АНБ) (более подробно мы расскажем об этом чуть ниже). По всей видимости, компания рассчитывает с помощью АНБ обезопасить свою сеть, которая недавно подверглась атакам китайских хакеров.

Создание таких систем предполагает объединение усилий государства, частного сектора, неправительственных и международных организаций, что позволяет участникам использовать географические, технологические и информационные ресурсы, которые они не смогли бы освоить в одиночку. Однако возникновение новых систем управления связано с рядом теоретических и практических проблем, изучением которых никто до сих пор серьезно не занимался.

Теория комплексных систем управления еще недостаточно хорошо изучена. А на практическом уровне без ответа пока остаются множество вопросов, касающихся прозрачности, надзора и контроля, ответственности и подотчетности, а также стоимости (в широком смысле) новых систем управления и эффективности их использования в целях укрепления безопасности.

Особенно остро эти пробелы и проблемы ощущаются в случаях, когда государство привлекает для решения своих задач заинтересованные структуры частного сектора. Уже в силу самой своей природы государственно-частное партнерство не может быть полностью прозрачным, а деятельность участников системы часто состоит из множества различных видов, которые недоступны для надзора со стороны контролирующих организаций и органов демократического управления. Кроме того, как указывает А. Бейлс,

---

[9] Alyson Bailes, "Private Sector, Public Security," in *Private Actors and Security Governance*, ed. Alan Bryden and Marina Caparini (Berlin: Lit Verlag, 2006), 42.

> … баланс контроля в сфере государственно-частных отношений смещается в сторону безопасности[...] сегодня практически не бывает случаев, когда государство может просто заставить частный бизнес делать то, что ему нужно, и даже более очевидные методы опосредованного управления – от правового регулирования на национальном и международном уровнях до внедрения системы экономических стимулов – все сложнее применять в новой обстановке, где все большую роль начинают играть нетрадиционные, негосударственные, многонациональные и транснациональные силы и субъекты.[10]

В этом отношении больше всего беспокойства вызывает использование частных военных компаний и охранных предприятий. Но это далеко не единственная серьезная проблема, возникающая в контексте борьбы с кибер-угрозами. Существуют и ряд других проблем, которые осложняют решение задач надзора и контроля в сфере борьбы с кибер-угрозами и связанного с ней государственно-частного партнерства. Далее мы перечислим эти проблемы, а затем приведем несколько примеров из государственной практики Великобритании, США и Австралии.

Во-первых, проблема осуществления надзора осложняется ввиду *присутствия в системе множества различных участников*. Как мы увидим далее, в обеспечении кибербезопасности задействовано огромное количество самых разных структур – как государственных, так и частных и негосударственных, а также международных. Точно так же, огромное количество самых разных участников задействовано в том, что мы могли бы назвать общим термином «кибератаки». При такой сложности системы органы надзора, в частности, парламентские комитеты (возможности которых нередко весьма ограничены) не в состоянии эффективно отслеживать всех участников системы или получать сведения об их существовании и деятельности, а в некоторых случаях даже не могут получить на это соответствующие полномочия.

Во-вторых, проблема надзора усугубляется *недостатком соответствующих технических знаний и возможностей*. Ввиду очень сложной технической природы проблем кибербезопасности и средств их решения надзорным органам часто не хватает необходимого опыта для того чтобы их понять и правильно организовать процессы надзора. Проблема обостряется еще больше в случае государственно-частного партнерства, при котором создается своего рода барьер между высокооплачиваемыми и технически грамотными специалистами, участвующими в реализации правительственных директив, с одной стороны, и (часто) низкооплачиваемыми и не так хорошо технически подготовленными государственными служащими, которым поручено осуществлять надзор за их деятельностью, с другой стороны.

В-третьих, проблемы надзора усугубляются сложностями *правового характера*. Борьба с киберпреступностью ставит на повестку дня необходимость решения сложных правовых вопросов, связанных (в том числе) с соблюдением прав на неприкосновенность частной жизни и свободу выражения мнений. Проблема усложняется государственно-частным партнерством и связанными с этим правовыми вопросами, касающимися ответственности, подотчетности и контроля.

---

[10] Bailes, “Private Sector, Public Security,” 42.

В-четвертых, проблема надзора усугубляется *неоднородностью участников системы*. В большинстве случаев сфера ответственности надзорных органов определяется в зависимости от их принадлежности к тому или иному ведомству или возложенных на них задач. Например, парламентский комитет может осуществлять надзор за деятельностью разведывательных служб, вооруженных сил или органов юстиции. Однако государственно-частное партнерство в сфере кибербезопасности не ограничено рамками конкретных ведомств, и поэтому надзор за такой деятельностью выходит за пределы полномочий соответствующих контролирующих организаций. В результате во многих сферах деятельности надзор осуществляется очень слабо либо не осуществляется вообще.

В-пятых, проблема надзора усугубляется *отсутствием общих подходов к оценке сфер полномочий контролирующих организаций*. Например, государственные контролирующие организации, как правило, занимаются только теми ведомствами, которые непосредственно входят в сферу их компетенции. Это значит, что частные партнеры этих ведомств остаются вне зоны контроля, причем даже в тех случаях, когда их деятельность непосредственно финансируется из бюджета этих ведомств или если они тесно с ними взаимодействуют.

В-шестых, проблема надзора усложняется *разрывом связи между принципалом* (тот, кто доверяет исполнение некоторых из своих функций кому-то другому) *и агентом* (тот, кому доверено исполнение чьих-то определенных функций). Действия любого агента, действующего от имени государства, связаны вертикалью подчиненности, ведущей от принципала к агенту. Например, парижский полицейский через своего начальника связан с превотом (высшим офицером полиции), префектом (высшим должностным лицом полиции, назначенным правительством для осуществления политического руководства) и, наконец, с Министерством внутренних дел и исполнительной властью. Таким образом, инструменты демократического управления (например, парламент) и физические лица или ведомства, реализующие указания правительства, связаны между собой вертикалью подчиненности и надзора. Однако с внедрением в систему частных исполнителей и созданием механизмов государственно-частного партнерства эти связи нарушаются. Получившая государственный заказ частная компьютерная фирма может действовать просто как агент государства (принципала). Но на самом деле отношения между этими двумя сторонами могут быть намного сложнее. Свой отпечаток на них накладывает асимметрия самой разной информации (ассиметричная информация – информация, неравномерно распределенная между участниками сделки или иного экономического процесса), что снижает уровень прозрачности и не позволяет эффективно использовать весь потенциал механизмов надзора.

Поскольку для служб безопасности многих стран мира проблема обеспечения безопасности компьютерных сетей возникла относительно недавно, инструменты демократического контроля – в виде омбудсменов, парламентских комитетов и других специализированных органов – просто не успевают адаптироваться к новым задачам. Например, в Великобритании надзор за деятельностью правительства в сфере обеспечения кибербезопасности осуществляют органы межведомственного контроля, правительственный комитет по вопросам национальной безопасности, международных отношений и развития и его

подкомитет по вопросам безопасности и чрезвычайных ситуаций. Если Великобритания будет рассматривать вопрос кибербезопасности в одном ряду с более традиционными вопросами обороны, эффективность надзора в этой сфере может снизиться под влиянием таких факторов, как *недостаток соответствующих технических знаний*, *отсутствие общих подходов к оценке сфер полномочий контролирующих организаций* и *сложности правового характера*, которые уже были рассмотрены выше.

Похожая ситуация и в Австралии, где деятельность правительства по борьбе с киберпреступностью контролируют уже существующие органы и комитеты, в частности (в сферах, где задействованы разведывательные службы) Генеральный инспектор служб разведки и безопасности и Объединенный парламентский комитет по вопросам разведки и безопасности. При такой схеме на эффективность надзора могут повлиять проблема *неоднородности участников системы противодействия кибер-угрозам* и *отсутствие общих подходов к оценке сфер полномочий контролирующих организаций*.

Несколько лучше ситуация в США, но и там есть сферы деятельности, которые пока остаются вне зоны доступа для органов надзора. В штате отдела Гражданских свобод и частных прав (Civil Liberties and Privacy Office – CLPO) при Управлении директора национальной разведки (УДНР) появилась должность заместителя начальника по вопросам гражданских свобод. В его задачи входит надзор за тем, чтобы соблюдение федеральных юридических норм и обеспечение прав американцев на неприкосновенность частной жизни находили должное отражение в общих подходах УДНР и различных разведывательных структур США к сбору и обработке персональной информации и строго соответствовали Конституции и законодательству США. При этом надзорные функции, в частности на уровне Конгресса, осуществляют, по крайней мере, четыре уполномоченных комитета и столько же подкомитетов, отвечающих за контроль над бюджетом. Каждый из комитетов может по-своему рассматривать эту проблему и при решении вопросов пытаться сместить баланс в сторону интересов собственной деятельности. Как и при решении многих других вопросов, связанных с *неоднородностью структуры участников* той или иной системы, раздробленность системы надзора может помешать усилиям по созданию единого подхода к решению проблемы. К примеру, Google и АНБ недавно объединили свои возможности в сфере борьбы с кибер-угрозами. Такое решение было принято после серии масштабных кибер-атак на сети всемирной поисковой системы, которые предположительно осуществлялись с территории Китая. В статьях на эту тему, которые публиковала *Washington Post*, сообщалось, что это сотрудничество задумывалось в расчете на то, что «обе организации смогут осуществлять обмен критической информацией, не нарушая при этом политики Google и законов о защите конфиденциальности электронной переписки американских граждан».[11] Однако при этом не совсем понятно, насколько эта гарантия будет обеспечена любым из существующих механизмов демократического контроля, и в какой степени гарантии такой защиты будут обеспечены в отношении граждан других государств.

---

[11] Ellen Nakashima, “FBI Director Warns of ‘Rapidly Expanding’ Cyberterrorism Threat,” *The Washington Post*, 4 марта 2010 г.

2.2. Борьба с кибер-угрозами в контексте соблюдения гражданских прав и свобод

Сегодня угрозы кибербезопасности развиваются гораздо быстрее, чем возможности надзорных и регуляторных органов по выявлению нарушителей и привлечению их к ответственности. Эта тенденция вызывает особое беспокойство, если рассматривать ее в контексте возможных нарушений прав граждан на неприкосновенность частной жизни, свободу слова и свободу объединений.

Одним из ключевых компонентов стратегии кибербезопасности, который используют как правительства, так и физические лица и структуры частного сектора, является использование межсетевых (или защитных) экранов. Межсетевой защитный экран служит барьером между двумя или несколькими сетями и регулирует трафик между сетями согласно комплексу различных правил и ограничений.

На самом базовом коммерческом уровне, использование таких средств защиты предполагает государственно-частное партнерство, поскольку, как мы уже говорили, как правило, именно частные фирмы занимаются разработкой аппаратного и программного обеспечения, необходимого для создания технологий межсетевой защиты. Можно предположить, что партнерство в этой конкретной сфере будет активно развиваться и далее, учитывая, что правительства стран всего мира стремятся максимально расширить сферу применения технологий, использующихся сегодня для обеспечения безопасности сверхсекретных сетей, и внедрить их и на уровне других министерств и ведомств.[12]

Однако на более высоком уровне отношения между государственными и частными субъектами подпадают под действие сложных регуляторных норм, касающихся, в частности, электронной защиты критической инфраструктуры. Учитывая разнообразие субъектов, владеющих или иным образом участвующих в управлении объектами критической инфраструктуры (в том числе электростанциями, больницами, аэропортами и пр.), очевидно, что стратегия кибербезопасности не может ограничиваться только лишь рамками государственных информационных сетей. Уже даже ведутся разговоры о необходимости создания «системы межсетевой защиты, которая бы обезопасила все американские компьютеры в сети».[13] Но очевидно, что выбор подобной стратегии только приведет к «гонке вооружений межсетевой защиты», которая не даст ожидаемых результатов, особенно, если учесть, что (как показано в предыдущем примере) такая защита осуществляется только на уровне каждого отдельного государства, но не в глобальном масштабе. Как справедливо отмечает индийский эксперт в области законодательства по вопросам кибербезопасности Паван Даггал, ограниченность сферы действия национального зако-

---

[12] Ryan Singel, “Report: Government’s Cyber Security Plan is Riddled With New Spying Programs,” *Wired*, 15 мая 2008 г., Threat Level.

[13] Там же.

Таблица 4. Цензура в Интернете [14]

Согласно данным Инициативы OpenNet, по уровню цензуры в Интернете все государства можно условно разделить на три группы	
Очень высокий уровень цензуры	Бирма (Мьянма), Китай, Куба, Египет, Иран, Северная Корея, Саудовская Аравия, Сирия, Тунис, Туркменистан, Узбекистан, Вьетнам
Средний уровень цензуры	Австралия, Бахрейн, Южная Корея, Объединенные Арабские Эмираты, Йемен
Низкий уровень цензуры	Беларусь, Бельгия, Бразилия, Канада, Чили, Хорватия, Чешская Республика, Дания, Эстония, Фиджи, Финляндия, Франция, Германия, Гана, Ирландия, Индия, Израиль, Италия, Иордания, Малайзия, Марокко, Нидерланды, Новая Зеландия, Норвегия, Пакистан, Польша, Россия, Сингапур, Словения, Швеция, Таиланд, Турция, Великобритания, Соединенные Штаты Америки

нодательства позволяет обеспечить «лишь частичную защиту пользователей средств трансграничной коммуникации».[15]

Попытки создания систем межсетевой защиты национального масштаба (или аналогичных систем для контроля международных информационных потоков) зачастую наталкиваются на ожесточенное сопротивление со стороны частных пользователей, а их сотрудничество с властями в этой области нередко имеет вынужденный характер. Например, нынешнее правительство Австралии предложило на рассмотрение парламента законопроект, обязывающий интернет-провайдеров блокировать доступ к определенным сайтам и категориям контента, что вызвало бурю протеста со стороны как коммерческих пользователей, так и гражданского общества. В частности, Google заявила о том, что предложенный законопроект является «слишком жестким и ограничивает право пользователей на доступ к информации». Кроме того, по мнению руководства компании, «Даже если такой контент и имеет непристойное содержание, то и в таком случае правительство не должно иметь права на ограничение доступа к информации, которая может послужить основой для обсуждения резонансных вопросов».[16]

Кроме того, рассредоточение ответственности, что часто происходит при государственно-частном партнерстве, может иметь прямые последствия, в том числе, и с точки зрения защиты прав человека. Когда государство и структуры частного сектора совместно решают задачи в сфере обеспечения законности и правопорядка, становится очень трудно найти виновных и привлечь их к ответственности в случае, если, например, имело место нарушение прав человека. Так, в США уже давно тянется дело телекоммуникационной корпорации

---

14 OpenNet Initiative, “Country Profiles,” *OpenNet*, http://opennet.net/research/profiles.

15 Pavan Duggal cited in William Maclean, “Cyber Evil Will Thrive Without Global Rules – Good Luck With That,” *Wired*, 22 февраля 2010 г., Epicenter.

16 Google, “Our views on Mandatory ISP Filtering,” *Official Google Australia Blog: News and Notes from Google Down Under*, 16 декабря 2009 г.

AT&T, которая обвиняется в предоставлении Агентству национальной безопасности (АНБ) огромного количества проходящих по ее каналам информации (электронные письма, телефонные звонки и т.д.) без соответствующей санкции судебных органов. В процессе судебного разбирательства до сих пор не удалось установить обвиняемого, так как ни предприятия телекоммуникационной корпорации, ни правительство своей вины в этой ситуации не признают.[17] (см. Вставку 1).

Еще одна проблема состоит в том, что совершенствование возможностей по идентификации и авторизации пользователей в корне противоречит интересам защиты права человека на неприкосновенность частной жизни. Задача обнаружения киберпреступников связана с большими сложностями, для решения которых требуются специфические технические знания и опыт. Эта особенность борьбы с кибер-угрозами порождает еще одну проблему, которая состоит в том, что в целях обеспечения собственной безопасности (и безопасности своих клиентов) государства и частные компании собирают и обрабатывают огромное количество персональных и конфиденциальных данных, причем во многих случаях это происходит без надлежащего демократического контроля. Так, недавно назначенный на должность руководителя Кибернетического командования (United States Cyber Command – подразделение вооружённых сил США, отвечающее за безопасность военных информационных сетей) генерал-лейтенант Кит Александр недавно заявил на заседании Сенатского комитета по делам Вооруженных сил, что данные о влиянии новых мер информационной безопасности на частную жизнь граждан «разглашению не подлежат».[18]

Для оперативной идентификации хакеров и киберпреступников предпринимаются и предлагаются самые разные меры. Так, Американское агентство перспективных оборонных разработок (DARPA) разработало проект создания так называемого «кибергенома», который позволит отслеживать происхождение документов и кодов. Этот проект является своего рода современным аналогом технологии времен Второй мировой войны, когда радистов можно было легко обнаружить по их «почерку» при передаче сообщений азбукой Морзе, даже если они пользовались при этом каналами защищенной связи.[19] Менее радикальные решения предусматривают меры, которые бы законодательно обязывали Интернет-провайдеров в течение нескольких лет сохранять данные своих клиентов, в том числе и аккаунты динамических IP-адресов в каждый конкретный период времени.

---

[17] David Kravets, “Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping,” *Wired*, 29 января 2010 г., Threat Level.

[18] Steven Aftergood, “Privacy Impact of Internet Security is Classified, NSA Says,” *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, 21 апреля 2010 г.

[19] Noah Shachtman, “’Don’t Be Evil,’ Meet ‘Spy on Everyone’: How the NSA Deal Could Kill Google,” *Wired*, 4 февраля 2010 г, Danger Room.

Вставка 1. Неподсудность телекоммуникационных компаний [20]

В июне 2008 года Палата представителей США приняла закон, которым предоставляется иммунитет от судебного преследования ряду американских телекоммуникационных компаний, в том числе AT&T и Verizon. Этот иммунитет защищает их от судебного преследования по более чем четырем десяткам исков, связанных с их участием в государственных программах администрации Дж. Буша, которые предусматривали ведение контроля за электронной перепиской и интернет-трафиком без соответствующей санкции суда. В исковых заявлениях утверждается, что указанные фирмы нарушали законы о частной жизни и способствовали ведению шпионской деятельности без разрешения судебных органов.

Этот закон, а также действия американских телекоммуникационных компаний, которые привели к его принятию, ставят на повестку дня ряд важных вопросов об ответственности частных субъектов государственно-частного партнерства в области борьбы с киберпреступностью. В связи с этим Глава юридического комитета Сената Патрик Лихи отметил: «Я совсем не хочу, чтобы пострадали телекоммуникационные компании. Я поддержал бы предложение о том, чтобы государство оградило их от ответственности или взяло на себя их ответственность по этим судебным искам [...], потому что лично я считаю, что ответственность все равно должна быть».[21]

В частности, Европейский Суд по правам человека в ходе рассмотрения дела 2008 года (истец – гражданин К.У. против Финляндии) пришел к выводу о том, что существует достаточно правовых оснований для удовлетворения запросов государственных органов стран-членов Совета Европы на предоставление информации от интернет-провайдеров, если это требуется для расследования уголовных дел.[22]

При обосновании своего решения Суд привел несколько примеров из европейского законодательства и практики правоприменения, в том числе Рекомендации Кабинета министров Совета Европы № R (95) 13 о применении уголовно-процессуального законодательства по отношению к преступлениям в сфере информационных технологий, а также Европейскую Конвенцию о борьбе с киберпреступностью. В обоих этих документах содержатся положения, обязывающие провайдеров интернет-услуг предоставлять по требованию компетентных следственных органов информацию, необходимую для идентификации пользователей услуг.[23] Суд также сослался на Статью 5 Директивы ЕС 2002/58/ЕС, которая гласит: «Государства-члены обеспечивают сохранение следующих категорий данных в соответствии с настоящей Директивой: (а) данные, необходимые для отслеживания и идентификации источника связи [...]; (2) касающиеся доступа в Интернет, электронной почты и Интернет-телефонии [...]; (3) имя, фамилия и адрес абонента или зарегистрированного пользователя, которому во время сеанса связи был присвоен тот или иной ад-

---

[20] Elana Schor, “Telecoms Granted Immunity in US Wiretapping Probe,” *The Guardian*, 20 июня 2008 г.

[21] KU v. Finland [2008] ECHR 2872/02.

[22] Там же.

[23] Там же.

рес Интернет-протокола (IP), идентификатор пользователя или номер телефона».[24]

Однако эти тенденции испытывают определенное давление с противоположной стороны. Так, в 2008 году Группа европейских адвокатов, известная как «Article 29 Data Protection Working Party», потребовала объяснить, зачем компании Google необходимо хранить конфиденциальную информацию о пользователях и сведения об их поисковых запросах, а также доказать, что Google выполняет все необходимые требования по защите данных. В интервью Reuters Комиссар ЕС по вопросам юстиции Жак Барро заявил, что решение компании о сокращении сроков сохранения анонимности IP адресов и куки-данных (используются веб-серверами для различения пользователей и сохранения данных о них) с 18-ти до 9-ти месяцев было «шагом в правильном направлении», но его все же недостаточно для защиты конфиденциальных данных о пользователях поисковика Google.

Проблема борьбы с киберпреступностью в значительной мере усложняется ввиду глобальных масштабов информационных сетей. В данном случае эффективности предпринимаемых усилий мешают те же проблемы, которые присущи любому кооперационному проекту международного уровня. Кроме того, возникают и дополнительные сложности, связанные с участием структур частного сектора (см. вставку 2). Если какой-то вебсайт с вредоносным контентом имеет расширение, например, *.ch* (Швейцария), но принадлежит России и размещен при этом в Нидерландах, то кто в таком случае несет за него ответственность, и какие правовые нормы должны при этом применяться? Но даже ответ на этот главный вопрос, т.е. кто конкретно стоит за тем или иным IP-адресом, требует участия субъектов частного сектора, многие из которых либо вообще не хранят подобную информацию, либо не хотят ею делиться из боязни отпугнуть или потерять клиентов.

Эта проблема усугубляется еще и тем, что во многих странах законодательство по этому вопросу либо вовсе отсутствует, либо имеет очень ограниченный характер. Во многих случаях, даже если руководство страны решительно настроено на борьбу с киберпреступностью, у государства нет необходимых технических возможностей для разработки нужного законодательства или его эффективной реализации в случае, если такое законодательство уже существует. В условиях отсутствия необходимой нормативно-правовой базы и технических возможностей для ее реализации, преступники могут войти в Интернет анонимно, пользуясь сетью на территории слабо развитого государства (например, при помощи незарегистрированной SIM-карты) и безнаказанно совершать свои преступления из-за рубежа.[25] По словам председателя консультативного совета Международного многостороннего партнерства против киберугроз (международная организация, действующая под эгидой ООН) Датука Мухаммеда Нур Амина, такие страны рискуют превратиться в «недееспособные государства киберпространства» (cyber failed states).[26] Учитывая затрат-

---

[24] Из материалов дела «KU v. Finland» [2008] ECHR 2872/02.

[25] Maclean, "Cyber Evil Will Thrive Without Global Rules – Good Luck With That."

[26] Noor Amin cited in Maclean "Cyber Evil Will Thrive Without Global Rules – Good Luck With That."

ность мероприятий по обеспечению безопасности информационных сетей (по различным оценкам, от 3 до 10 % от общих расходов на содержание сетей), непонятно, как скоро такие государства смогут овладеть необходимыми ресурсами.

Поэтому необходимо создать общую стратегию и общие правовые нормы, которые бы регулировали правила борьбы с кибер-угрозами на международном уровне. Однако усилия по развитию международного сотрудничества в этой сфере неизбежно потребуют решения такой серьезной проблемы, как соблюдение оптимального баланса между требованиями о сохранении анонимности, конфиденциальности и открытости, с одной стороны, и требованиями кибербезопасности, с другой стороны, в частности, что касается информационных обменов и совершенствования возможностей по поиску киберпреступников. Например, уже описанная выше технология, которую предлагает агентство DARPA, могла бы пригодиться репрессивным политическим режимам, стремящимся сохранить свою монополию на власть. По мнению экспертов Центра демократии и технологий, даже само хранение в базах интернет-провайдеров данных об их клиентах «является посягательством на их личную жизнь; оно не нужно и вряд ли даст ожидаемый эффект».[27] Кроме того, во многих странах надзор в этой сфере осуществляется для того, чтобы не позволить государству злоупотреблять своим правом на получение информации, позволяющей установить личность пользователя и его действия в сети, по причинам, о которых мы уже говорили в предыдущем разделе.

Как было отмечено в недавнем докладе Центра стратегических и международных исследований (CSIS), «анонимность, а в большинстве случаев и невозможность точно установить личность пользователя сети действительно создают ряд серьезных проблем при борьбе с кибер-угрозами, но они же могут служить защитой для пользователей, которые, к примеру, хотят высказать альтернативную точку зрения, не совпадающую со взглядами остальной части общества».[28] В докладе предлагается распределить виды деятельности в интернете по категориям в зависимости от степени риска для безопасности сети, где на самой нижней ступени будут, например, интернет-магазины и им подобные ресурсы (низкий уровень риска), а на самом верху пирамиды – виды деятельности, связанные с доступом к системам управления объектами критической инфраструктуры. Таким образом, физические лица смогут свободно пользоваться определенными ресурсами, для которых будет установлен низкий уровень требований относительно идентификации пользователя, но при использовании ресурсов, связанных с более высоким уровнем риска, пользователи должны будут предоставлять достоверные данные, подтверждающие их личность и право на доступ к соответствующим ресурсам.[29]

---

[27] Julian Sanchez, “New Bill Would Force ISPs to Retain User Data for Two years,” *Ars Technica*, 19 февраля 2009 г.

[28] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington DC: CSIS, 2008).

[29] Там же.

Вставка 2. Международное сотрудничество и ботнет-сеть Mariposa

В мае 2009 года частная канадская охранная фирма Defense Intelligence обнаружила гигантскую бот-сеть под кодовым наименованием Mariposa, которая за время своей деятельности успела заразить свыше 13 миллионов компьютеров в более чем 190 странах мира. Среди инфицированных машин оказались компьютеры крупных банков и более половины крупнейших компаний мира из списка Fortune 1000.

Ботнет-сеть Mariposa, управляющие центры которой находились на территории Испании, специализировалась на хищениях персональных идентификаторов к веб-аккаунтам, а также банковских реквизитов и реквизитов кредитных карт. Кроме того, части зомби–сети сдавались в аренду различным организованным преступным группировкам.

После обнаружения сети Defense Intelligence активно сотрудничала с испанской фирмой Panda Security, а также со специалистами ФБР США и испанской полиции. В результате их совместных действий удалось установить личности и арестовать операторов сети, а саму сеть – ликвидировать.

2.3. Средства сдерживания и противодействия в кибер-войне

Одно из последствий вышеописанной проблемы, а именно сложности, связанные с установлением источника угрозы, состоит в том, что в данном случае невозможно полноценно применять традиционные средства сдерживания и противодействия. Если очень трудно определить источник атаки, то так же трудно будет и сдерживать дальнейшие атаки, например, угрозой применения ответных действий.[30]

Ученые, занимающиеся исследованиями по вопросам войны в киберпространстве, пришли к выводу, что в данном случае обладание большим наступательным потенциалом почти никак не сказывается на уровне оборонного потенциала. Эксперт Центра стратегических и международных исследований Джеймс А. Льюис отмечает: «Широко известно, что США обладают мощнейшими в мире возможностями для ведения наступательных действий в кибервойне, но это не дает практически никакого эффекта с точки зрения сдерживания возможных атак».[31] Конечно, ученые когда-нибудь придут к созданию надежных средств сдерживания, но на данном этапе, как свидетельствуют последние события в киберпространстве, создание технологий нападения явно опережает усилия по созданию эффективных технологий сдерживания. Как сказал в своей статье в Нью-Йорк Таймс Джозеф Най, «сейчас мы находимся в той же фазе, в которой оказались в начале 1950-х, когда СССР обзавелся ядерной бомбой [...]; это будет не совсем то, чем были ядерные средства устрашения, но [...], по крайней мере, мы можем увеличить затраты нападающей стороны».[32]

---

30 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Washington DC: RAND, 2009).

31 Markoff, Sanger, and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent."

32 Цитата заимствована из Markoff, Sanger, and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent."

Еще одна проблема заключается в том, что даже если и удается точно установить источник атаки, при этом не всегда можно применить адекватные меры противодействия. Отчасти это объясняется огромными сложностями, связанными с надежным разграничением ответственности за такие преступления, как вандализм, хищение коммерческой собственности или поддерживаемые государством военные действия в киберпространстве.[33] Кибервойна стирает различия между разными категориями нападающих, и точно так же она стирает различия между военными и гражданскими объектами атак. Так, например, кибертеррористы могут вызвать настоящий хаос в стране, направив свою атаку на ее финансовую систему, и при этом им даже не придется атаковать военные или государственные объекты.[34]

Это обстоятельство создает серьезные проблемы для тех, кто разрабатывает ответные действия. Статья 2 (4) Устава ООН гласит: «Все Члены Организации Объединенных Наций воздерживаются в своих международных отношениях от угрозы применения силы или ее использования как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с Целями Организации Объединенных Наций». Этот принцип, который сегодня является частью международного права, запрещает применение силы при любых обстоятельствах, за исключением двух заранее определенных ситуаций. Во-первых, Совет Безопасности может дать санкцию на осуществление коллективных действий с целью поддержания или обеспечения международного мира и безопасности; и, во-вторых, государства могут действовать в порядке «индивидуальной или коллективной самообороны в случае вооруженного нападения на какое-либо из государств». Комментируя атаки на серверы государственных учреждений Эстонии (см. вставку 3), Яак Аавиксоо, в то время занимавший пост Министра обороны Эстонии, заметил:

> В настоящее время НАТО не рассматривает хакерские атаки как явно военные действия. Это означает, что Положения статьи V Североатлантического договора, или, другими словами, коллективной самообороны, не будут автоматически распространяться на страну, которая подверглась нападению [...] сегодня ни один Министр обороны НАТО не определил бы кибератаку как сугубо военное действие. Тем не менее, этот вопрос требует решения уже в самом ближайшем будущем.[35]

Между тем продолжаются споры о том, какие надежные и в то же время законные меры противодействия может предпринять государство в случае массированных хакерских атак. То есть следует определиться, в каких случаях это должен быть дипломатический демарш, официальный протест или введение экономических санкций, а в каких привлечение к уголовной ответственности

---

[33] Markoff, Sanger, and Shanker, “In Digital Combat, U.S. Finds No Easy Deterrent.”

[34] Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyberpower and National Security* (Washington DC: Center for Technology and National Security Policy, National Defence University, 2009).

[35] Jaak Aaviksoo, цитата приведена в статье Ian Traynor, “Russia Accused of Unleashing Cyberwar to Disable Estonia,” *The Guardian*, 17 мая 2007 г.

Вставка 3. «Кибервойна» против Эстонии [36]

Эстония входит в число мировых лидеров по уровню развития электронных технологий, и правительство этой страны переводит все больше видов своей деятельности в виртуальное пространство. Заседания на уровне Кабинета министров проходят в онлайн-режиме, а граждане Эстонии могут голосовать на общенациональных выборах с помощью своих компьютеров. В 2007 году Эстония занимала 23-е место в мировом рейтинге по уровню компьютеризации (e-readiness Ranking). Почти 61 процент населения имеет электронный доступ к своим банковским счетам, а 95 процентов всех банковских операций осуществляются в электронном формате.

Однако такой высокий уровень компьютеризации имеет и свою обратную сторону. В апреле 2007 года сайты эстонского парламента, министерств и ведомств, банков и средств массовой информации подверглись серии массированных и хорошо скоординированных распределенных атак на отказ в обслуживании (DDoS-атаки). Перенос памятника советскому Воину-освободителю из центра Таллинна на окраину вызвал волну протестов среди русскоязычного населения страны, которые вылились в массовые уличные беспорядки. За этими протестами последовала серия DDoS-атак на серверы эстонских госучреждений. В результате клиенты не могли получить доступ к этим сайтам, а некоторые из них оказались полностью заблокированными. В российских интернет-чатах тут же появились призывы к активным действиям, которые сопровождались подробными инструкциями для желающих принять участие в DDoS-атаках. В результате веб-сайты Министерств иностранных дел и юстиции были закрыты, а сайт Партии реформ, возглавляемой действующим премьер-министром Андрусом Ансипом, полностью вышел из строя. На время оказались заблокированными и телефонные линии служб по чрезвычайным ситуациям. Перманентные атаки на серверы государственных учреждений, в том числе Государственной канцелярии и Федеральной избирательной комиссии, продолжалась с небольшими перерывами до середины мая 2007 года.

Эксперты по-разному оценивали масштабы и последствия этих кибер-атак. В ходе предварительного расследования выяснилось, что часть компьютеров, с которых осуществлялись DDoS-атаки, была расположена в России, причем ряд IP-адресов указывали на компьютеры, находящиеся в госучреждениях РФ. Как и в любом другом преступлении в интернете, в данном случае проблема заключалась в том, что, даже после того, как был установлен источник нападения, эффективно защититься от этих атак было невозможно. Несмотря на некоторые достаточно любопытные заявления, сделанные в то время, сейчас принято считать, что атаки на эстонские сети не имели признаков настоящей «кибервойны», а были, скорее, «киберконфликтом локального характера». Конечно, для такого небольшого государства, как Эстония, они создали серьезные проблемы. Но эти атаки были достаточно примитивными с технической с технической точки зрения, и поэтому на них нельзя строить оценки относительно характера будущей киберовойны. Эстонская компьютерная группа экстренной готовности (как и в большинстве других государств, такие

---

[36] Некоторые из материалов для этой вставки были любезно предоставлены г-ном Фредом Шрайером. Также см. Cyrus Farivar, “Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat,” *Slate*, 22 мая 2007 г.; Johnny Ryan, “iWar: A New Threat, Its Convenience – and Our Increasing Vulnerability,” *NATO Review*, Winter 2007; Shaun Waterman, “Who Cyber Smacked Estonia?” *United Press*, 11 июня 2007 г.; Kevin Poulsen, “‘Cyberwar’ and Estonia’s Panic Attack,” *Wired*, 22 августа 2007 г., Threat Level; Singel, “Report: Government’s Cyber Security Plan is Riddled With New Spying Programs.”

органы занимаются координацией действий государственных и частных структур в вопросах противодействия интернет-угрозам) оперативно и грамотно отреагировала на эти атаки, используя пакетную фильтрацию и другие устоявшиеся и успешные методики.

Многие указывали на события в Эстонии лишь как на предвестие гораздо более серьезных и разрушительных сражений будущего. Но высказывались и другие точки зрения. В частности, многие предупреждали о том, что, преувеличивая последствия атак, подобных эстонской, можно скатиться в другую крайность, а именно в направлении большей закрытости интернета. Возможно, это и облегчит задачу обнаружения киберпреступников. Однако, с другой стороны, при этом могут оказаться под угрозой такие фундаментальные права человека, как право на неприкосновенность частной жизни и право на свободное высказывание своих мнений. В частности, бывший директор национальной разведки США Майкл Макконнелл предлагает «модернизировать Интернет с тем, чтобы упорядочить управление процессами установления авторства, определения географического положения, анализа полученной информации и оценки возможных последствий». Однако подобные меры приведут к тому, что государство фактически получит возможность вмешиваться в личную жизнь граждан, следя за тем, о чем они пишут в своей электронной переписке, какие запросы вводят в поисковые системы и какой контент загружают с веб-сайтов.

или военный удар.[37] Создание в Таллинне Объединенного центра обмена передовым опытом в сфере компьютерной обороны НАТО (Cooperative Cyber Defense Centre of Excellence/CCDCOE), главная задача которого состоит в совершенствовании методов противодействия кибер-угрозам, позволяет предположить, что Альянс расценивает хакерские атаки на эстонские сети как начало масштабной кибервойны. В подтверждение этого предположения, на вебсайте CCDCOE говорится, что «Современные вооруженные силы готовятся к использованию киберпространства в качестве параллельного плацдарма для ведения сражений во время будущих конфликтов [...] Даже при низкой вероятности чисто сетевых атак, кибератаки, организованные в комплексе с применением обычных вооружений, станут стандартным оперативным компонентом военных действий будущего».[38] Многие государства мира уже вступили в гонку за обладание техническими возможностями, которые позволят им участвовать в этой «революции военного дела». Но это означает, что такими же активными должны быть и усилия по созданию правовых норм и структур, регулирующих вопросы прозрачности, ответственности и контроля в этой сфере.

В контексте борьбы с кибер-угрозами существует и целый ряд других проблем демократического управления. Во-первых, это проблема рассредоточения ответственности. Иными словами, достаточно часто бывает трудно определить ответственного за ту или иную сферу деятельности, возникшей в результате слияния различных функций, каждой из которых раньше занимались отдельные структуры. Поэтому необходимо каким-то образом связать воедино различные функции, ведомства и механизмы реагирования на угрозы, которые

---

[37] Jeffrey Carr, “Responding to International Cyber Attacks as Acts of War,” in *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O’Reilly Media, 2010).

[38] Cooperative Cyber Defence Centre of Excellence, “General Trends,” www.ccdcoe.org/8.html.

прежде функционировали отдельно друг от друга. Особенно это касается искусственного разделения функций и обязанностей между ведомствами, занимающимися вопросами национальной безопасности, и другими государственными структурами. Это же относится и к сфере законодательного обеспечения, где существует комплекс не связанных между собой законов, которые принимались для регулирования изначально различных сфер деятельности. Сегодня как никогда важно четко распределить роли и обязанности как внутри государственных и частных субъектов борьбы с кибер-угрозами, так и между ними.[39]

Во-вторых, субъекты этой деятельности зачастую крайне неохотно делятся полученной информацией. Это вызывает все большую озабоченность политиков, особенно учитывая большое количество субъектов, в распоряжение которых попадает информация, требующая безотлагательного принятия решений. Приведем лишь один пример. Для того чтобы защитить свои ценные ноу-хау, компании предпочитают держать в секрете информацию о своих мерах безопасности до тех пор, пока они не начнут их открыто применять. Это приводит к тому, что все недостатки таких мер выявляются только после того, как сами меры уже приняты.[40] Во многих случаях государство получает возможность узнать о факте нападения только тогда, когда оно само становится очевидной мишенью киберпреступников. Так, комментируя недавние хакерские атаки на поисковую систему Google, один из высокопоставленных сотрудников разведки признал, что «если бы представители Google не сообщили нам, что их компания и другие фирмы подверглись кибер-атакам, то мы бы, наверное, никогда бы о них и не узнали. Такая ситуация просто недопустима».[41] С другой стороны, государство может не знать и о том, что его собственная территория может служить плацдармом для осуществления кибер-атак физических или юридических лиц.

Для решения этой проблемы предлагаются несколько путей. Один из них предусматривает обязательное информирование государственных органов обо всех фактах кибер-атак, если их количество превышает определенное установленное пороговое значение. Однако, учитывая, что большой совокупный эффект может быть достигнут и в результате огромного количества относительно безобидных атак, пока непонятно насколько предлагаемая мера окажется эффективной в конечном итоге. В свою очередь, Великобритания внедрила у себя систему поощрения информационных обменов, при которой никто, кроме первоначального владельца, не имеет права распоряжаться полученной информацией. Это значит, что информация передается не правительству, а уполномоченным структурам по защите информационной безопасности, и именно они осуществляют анализ и интеграцию полученных данных.[42] При этом для частных субъектов первостепенное значение имеют вопросы доверия и прозрачности, так как, если правительство заставит их предоставлять слишком большие объемы информации, например, о своих клиентах и т.д., они

---

39 White House, *Cyberspace Policy Review*.

40 Jim Giles, "Benevolent Hackers Poke Holes in E-Banking," *New Scientist*, 29 января 2010 г.

41 Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent."

42 White House, *Cyberspace Policy Review*.

могут их потерять, а, следовательно, и утратить свои позиции на рынке. С другой стороны, они, так же, как и правительство, не хотят стать объектами кибер-атак и поэтому заинтересованы в сотрудничестве с целью разработки эффективных мер противодействия. Кроме того, существует и множество нерешенных вопросов правового характера. В частности, это касается концентрации полномочий, определения полномочий правительства в сфере защиты находящихся в частных руках объектов критической инфраструктуры, размещения программных средств контроля и датчиков автоматического обнаружения и предупреждения об атаке, а также обмена данными с третьими лицами и правовой защиты ответственности частных субъектов.

Другое предложение предусматривает создание на уровне государства мощных структур, в которые бы стекалась вся информация от различных субъектов (таких, как местные центры кибербезопасности) с целью разработки целостной картины киберугроз и состояния сети, а также координации действий при организации мер оперативного реагирования. На правительственном уровне координация действий должна осуществляться совместно с правоохранительными структурами, органами разведки и контрразведки, а также вооруженными силами, и охватывать весь спектр вопросов – от внешних атак, действий пользователей сетей и выявления слабых мест в системах защиты,[43] до планирования мер по выявлению, сдерживанию и ликвидации угроз. Эти структуры должны быть интегрированы в единую комплексную систему, в частности, в таких аспектах деятельности, как реагирование на инциденты и создание систем сквозной защиты (т.е. именно в тех сферах, которыми сегодня никто не занимается).

Вставка 4. Грузинский конфликт [44]

Грузинский конфликт (2008 г.) уникален в том смысле, что именно тогда впервые в истории военные действия одной из сторон сопровождались массированными хакерскими атаками на серверы государственных и финансовых учреждений на территории противника. Российская киберблокада Грузии началась за несколько недель до начала полномасштабных боевых действий. Формальной причиной этой пятидневной войны была борьба Южной Осетии за независимость от Грузии и стремление Тбилиси вернуть контроль над мятежной республикой.

20 июля некоммерческая организация Shadowserver Foundation, осуществляющая мониторинг активности ботнетов в Сети, зарегистрировала серию DDoS атак на официальный сайт Президента Грузии Михаила Саакашвили. В результате президентский сайт более суток находился в режиме оффлайн. Эти атаки организовывались с сервера на территории США, что является еще одним свидетельством глобального характера кибер-угроз.

DDoS-атаки против неокрепшей интернет-инфраструктуры Грузии достигли своего пика 8-го августа, то есть в день начала боевых действий. В этот день эксперты Shadowserver впервые зарегистрировали атаки шести различных бот-сетей, кото-

[43] Там же.

[44] Материал для данной вставки был любезно предоставлен господином Фредом Шрайером.

рые была направлены на сайты грузинского правительства и средств массовой информации. Интенсивность атак российских хактивистов возрастала по мере эскалации конфликта. В результате на некоторое время прекратили свою работу сайты Президента, Парламента, Министерства обороны и Министерства иностранных дел, Национального банка Грузии и двух электронных информационных агентств.

Грузинское правительство отреагировало оперативно и творчески. На какое-то время сайты грузинского министерства иностранных дел и Civil.ge были размещены на сервисе Google Blogspot, где они были лучше защищены от атак, а 9 августа на серверы американской компании Tulip Systems, принадлежащей бизнесмену грузинского происхождения Нино Дояшвили, был перенесен и сайт президента Грузии Михаила Саакашвили. В знак солидарности Президент Республики Польша Лех Качиньский любезно предоставил место на своем сайте для размещения официальных пресс-релизов грузинского правительства. Ощутимую помощь оказало и Правительство Эстонии. В частности, оно разместило на своих серверах сайт Министерства иностранных дел Грузии и направило в страну двух специалистов по информационной безопасности, которые участвовали в модернизации системы кибероборонs Грузии.

Согласно выводам белорусского эксперта по вопросам хактивизма Евгения Морозова, координация атак осуществлялась с хакерского интернет-форума StopGeorgia.ru., который был основан уже через несколько часов после вторжения российских войск на территорию Южной Осетии. На форуме был выложен список вебсайтов-мишеней, который постоянно обновлялся, а для желающих присоединиться к DDoS-атакам прилагалась специальная бесплатная программа.

Существуют свидетельства и того, что при организации киберблокады Грузии использовались и более простые, но при этом не менее эффективные атаки типа SQL injection («SQL-вторжение» – один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода). Как правило, злоумышленники добиваются своей цели, отправляя на сервер миллионы бесполезных запросов, в результате сервер, обрабатывая их, перестает реагировать на запросы пользователей и фактически выходит из строя. С точки зрения хакера, SQL-атака обеспечивает два основных преимущества. Во-первых, при использовании в комплексе с традиционными DDoS-атаками SQL-атаку чрезвычайно трудно обнаружить и, во-вторых, SQL-атаки так же эффективны, как и DDoS–атаки, но достигают той же цели при использовании гораздо меньшего количества компьютеров.

В конечном итоге, эти кибератаки не нанесли значительного ущерба, поскольку большая часть экономики и объектов критической инфраструктуры Грузии пока находятся за пределами интернет-пространства. Однако, выведя Грузию в оффлайн, российские хакеры в каком-то смысле получили господство в Интернете. В самые критические дни боев российские СМИ могли представлять свое видение войны в то время, как грузины фактически оказались в условиях киберблокады.

Выводы

Из приведенного здесь анализа можно сделать несколько выводов. Во-первых, для организации эффективной борьбы с интернет-угрозами государство должно выйти за рамки чисто правительственного подхода и принять новый подход, во главу угла которого должно быть поставлено действенное государственно-частное партнерство. Так, например, правоохранительные органы не могут эффективно бороться с киберпреступностью в условиях, когда аналогичные функции и обязанности не сосредоточены у них в руках, а распределены среди целого ряда министерств и ведомств, а создание официальных сетей государственно-частного партнерства в этой сфере затруднено, либо эти сети функционируют неэффективно. Последнее обстоятельство имеет особое значение, учитывая, что обе стороны этого партнерства не склонны делиться важной информацией, особенно в случаях, когда дело касается международных и зарубежных компаний. В таком партнерстве должны быть задействованы не только частные субъекты, принимающие участие в так называемых «критических» сферах деятельности, но и фирмы, специализирующиеся в области информационной безопасности, а также разработчики программного обеспечения, производители оборудования, операторы сервисов электронных платежей и электронной почты, хостинг-провайдеры, участники банковского и финансового секторов, торговые Интернет-фирмы и физические лица.

Учитывая, что интернет-угрозы, как правило, имеют глобальный характер, возможно, придется организовать партнерство и на транснациональном уровне, где все проблемы проявляются даже острее, чем на уровне каждого конкретного государства. Вместе с тем, общие стратегии и принципы противодействия, выработанные региональными и международными субъектами, до сих пор остаются весьма поверхностными и малоэффективными. Проблема транснационального партнерства осложняется и ввиду огромных различий в возможностях разных государств (в данном случае имеются в виду техническая оснащенность, знания и опыт и, что особенно важно, нормативно-правовая база и механизмы надзора и контроля), и эти различия будут не уменьшаться, а только расти.

Во-вторых, из нашего анализа следует, что государственно-частное партнерство, без которого невозможно достижение всеобъемлющей и эффективной безопасности в киберпространстве, ставит на повестку дня целый ряд трудных вопросов, касающихся надзора, контроля и ответственности, прежде всего в сфере обеспечения таких фундаментальных прав человека, как право на неприкосновенность частной жизни, право на свободу высказываний и право на свободу объединения с другими людьми. Решение проблем кибербезопасности требует соблюдения оптимального баланса между интересами государства и личности (противоречие между которыми неизбежно присутствует при решении вопросов безопасности и во многих других сферах). К этому уравнению нужно добавить еще и третий важный компонент, а именно крупных субъектов частного сектора, каждый из которых руководствуется собственными мотивами и преследует собственные интересы. Отсутствие прозрачности создает множество трудностей в деятельности соответствующих надзорных органов, которые существуют далеко не везде.

В-третьих, вероятность развертывания масштабной кибервойны – помимо вопросов о том, каково будет ее влияние на общую тактику ведения боевых действий будущего – порождает целый ряд новых вопросов, касающихся мер государственного реагирования, демократического контроля и правового регулирования, которые возникают при необходимости отражения любого нападения. На каком этапе кибер-атака перерастет в кибервойну, и какие инструменты борьбы можно использовать при организации ответных действий – все эти вопросы, которые пока остаются без ответа, открывают совершенно новые направления в реформировании сектора безопасности и управлении сектором безопасности.

В нашей книге дается лишь краткий обзор этих вопросов. Как и во всех остальных книгах серии «Горизонт 2015», мы стремились поднять больше вопросов, чем предложить ответов.

Вот некоторые из этих вопросов:

- Каким образом можно контролировать развитие и выявление киберугроз (и совершенствовать уже существующие методы противодействия), не нарушая при этом принципов анонимности при использовании Интернета?
- Как можно усовершенствовать возможности и полномочия соответствующих контролирующих органов, которые позволили бы им эффективно осуществлять функции надзора в такой технически сложной и многосторонней сфере деятельности, особенно учитывая растущее влияние и роль спецслужб?
- При наличии разных уровней компьютеризации в США и Европе и огромной пропасти между странами-членами Организации экономического сотрудничества и развития (ОЭСР) и государствами развивающегося мира, как можно предупредить появление в киберпространстве недееспособных государств, и как можно усилить возможности стран Южного полушария в решении проблем нормативно-правового и технического обеспечения стратегий кибер-безопасности?
- Как государства могут обнаружить и ответить на такую новую угрозу, как война в киберпространстве? Очевидно, что здесь не обойтись без создания новых механизмов государственно-частного партнерства. Какими должны быть эти механизмы, насколько они должны быть прозрачны, и как лучше всего обеспечить надежный контроль над деятельностью этих механизмов со стороны законодательной власти и общества?
- Какова должна быть ответственность государства за кибер-атаки, организованные с его территории хакерскими группировками или отдельными лицами?
- Какой должна быть нормативно-правовая база, учитывая глобальный характер угрозы? Какие международные нормы и концепции применимы и необходимы в данном случае? Кто должен взять на себя инициативу в этом вопросе?
- В каком направлении должен развиваться Интернет: должен ли он оставаться открытой и демократичной системой, или будут сделаны шаги в

направлении, описанном Джорджем Оруэллом в его известном романе «1984»?

- Как можно в ходе публичных дискуссий достичь национального согласия по этим вопросам, сформировать стратегию и политику кибер-безопасности?
- Заменит ли кибервойна место кинетической энергии как главного средства поражения противника? Являемся ли мы невольными свидетелями второй волны революции в военном деле? Станет ли война в киберпространстве основным полем боя в будущих конфликтах? Если да, то какие последствия это будет иметь для вооруженных сил и сектора безопасности в целом? Какими будут эти последствия для разведывательных служб и правоохранительных органов?
- Играет ли время в нашу пользу? Не опережает ли технический прогресс развитие нормативной базы и стремление к демократическому контролю?

Ответы на эти и другие вопросы должны стать предметом дальнейшего и более детального анализа.

Список использованной литературы

Aftergood, Steven. "Privacy Impact of Internet Security is Classified, NSA Says." *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, 21 April 2010.

Arquilla, John and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age*. Washington DC: RAND, 1997.

Bailes, Alyson. "Private Sector, Public Security." In *Private Actors and Security Governance*, edited by Alan Bryden and Marina Caparini, 41-64. Berlin: Lit Verlag, 2006.

Carr, Jeffrey. "Responding to International Cyber Attacks as Acts of War." In *Inside Cyber Warfare: Mapping the Cyber Underworld*, 45-74. Sebastopol CA: O'Reilly Media, 2010.

Center for Strategic and International Studies. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington DC: CSIS, 2008.

Cooperative Cyber Defence Centre of Excellence. "General Trends." CCDCOE. http://www.ccdcoe.org/8.html (accessed 20 April 2010).

Farivar, Cyrus. "Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat." *Slate*, 22 May 2007.

Giles, Jim. "Benevolent Hackers Poke Holes in E-Banking." *New Scientist*, 29 January 2010.

Google. "Our views on Mandatory ISP Filtering." *Official Google Australia Blog: News and Notes from Google Down Under*, 16 December 2009.

Golumbic, Martin Charles. *Fighting Terror Online: The Convergence of Security, Technology, and the Law*. New York: Springer, 2007.

Kramer, Franklin D., Stuart H. Starr and Larry Wentz, eds. *Cyberpower and National Security*. Washington DC: Center for Technology and National Security Policy, National Defence University, 2009.

Kravets, David. "Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping." *Wired*, 29 January 2010, Threat Level.

KU v. Finland [2008] ECHR 2872/02.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Washington DC: RAND, 2009.

Lloyd's Emerging Risks Team. *Digital Risks: Views of a Changing Risk Landscape*. London: Lloyds, 2009.

Maclean, William. "Cyber Evil Will Thrive Without Global Rules – Good Luck With That." *Wired*, 22 February 2010, Epicenter.

Markoff, John, David E. Sanger and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *New York Times*, 25 January 2010, World section.

Nakashima, Ellen. "FBI Director Warns of 'Rapidly Expanding' Cyberterrorism Threat." *The Washington Post*, 4 March 2010.

OpenNet Initiative. "Country Profiles." OpenNet. http://opennet.net/research/profiles (accessed 20 April 2010).

Poulsen, Kevin. "'Cyberwar' and Estonia's Panic Attack." *Wired*, 22 August 2007, Threat Level.

Ryan, Johnny. "iWar: A New Threat, Its Convenience – and Our Increasing Vulnerability." *NATO Review*, Winter 2007.

Sanchez, Julian. "New Bill Would Force ISPs to Retain User Data for Two Years." *Ars Technica*, 19 February 2009.

Schor, Elana. "Telecoms Granted Immunity in US Wiretapping Probe." *The Guardian*, 20 June 2008.

Shachtman, Noah. "'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google." *Wired*, 4 February 2010, Danger Room.

Singel, Ryan. "Report: Government's Cyber Security Plan is Riddled With New Spying Programs." *Wired*, 15 May 2008, Threat Level.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, 17 May 2007.

United States Government Accountability Office. *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk*. Washington DC: US GAO, 2009.

Waterman, Shaun. "Who Cyber Smacked Estonia?" *United Press*, 11 June 2007.

White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington DC: White House, 2009.

Wood, Jennifer and Benoît Dupont, eds. *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, 2006.

Wulf, William A. and Anita K. Jones. "Reflections on Cybersecurity." *Science* 326 (13 November 2009): 943-4.

Приложение 1

ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ (ЗКИ/CIP), ЗАЩИТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ (ЗКИИ/CIIP) И КИБЕРБЕЗОПАСНОСТЬ

Краткий обзор организационных структур в некоторых странах [45]

Австралия. Вопросами ЗКИ/ЗКИИ занимается Центр оперативного управления кибербезопасностью. Основан в 2009 году в рамках государственной стратегии кибербезопасности и входит в состав Управления связи Министерства обороны (DSD/УСМО). В штат специалистов входят представители УСМО, Службы военной разведки, Вооруженных сил, Федеральной полиции и Службы безопасности и разведки Австралии. Информация о деятельности Центра находится по грифом секретности, однако известно, что Центр консультирует правительство по вопросам защиты страны от кибер-угроз и обеспечивает координацию действий путем интеграции знаний, опыта и разведданных.

В **Австрии** не существует единого органа, ответственного за ЗКИ/ЗКИИ. Каждое министерство и ведомство осуществляют собственные меры безопасности для защиты от внешних атак и предотвращения несанкционированного использования данных. Вопросами ЗКИИ занимаются несколько подразделений Министерства внутренних дел (BMI), в частности, в сфере обеспечения безопасности данных и борьбы с киберпреступностью. При Главном управлении общественной безопасности Федерального управления криминальной полиции работает информационный Центр по противодействию распространению детской порнографии. Федеральное Агентство государственной охраны и борьбы с терроризмом (BVT) отвечает за координацию вопросов безопасности личности и безопасности объектов. Второе Управление Министерства обороны занимается всеми направлениями информационной войны и при этом тесно взаимодействует с обеими спецслужбами. Одна из них, Abwehramt, имеет специальный департамент, занимающийся вопросами электронной обороны. Министерство транспорта, инноваций и технологий (BMVIT) отвечает за безопасность государственной информационной инфраструктуры. Оно же координирует работы в рамках национальной программы научных исследований и разработок в сфере безопасности. Если делать выводы на основании государственных программ в сфере кибербезопасности (программа электронного правительства, вебсайт государственной программы информационной безопасности, пилотный проект создания электронной интеллектуальной карты гражданина), в Австрии кибербезопасность в основном рассматривается в русле проблем защиты данных.

---

[45] Материалы для данного приложения были любезно предоставлены господином Фредом Шрайером.

Бельгия. За разработку государственной политики в сфере информационной безопасности отвечает Министерский комитет по вопросам безопасности, а вопросами реализации этой политики занимается Главное управление федеральной государственной службы по вопросам применения законодательства. Обеспечение безопасности персональных данных входит в сферу ответственности Комиссии по вопросам защиты частной информации. Бельгийский институт почтовых услуг и нарушений в сфере телекоммуникаций отвечает за реализацию и обеспечение соблюдения законодательства, касающегося электронной связи. Национальная компьютерная группа экстренного реагирования (CERT) до сих пор не создана, однако в штат оператора сети BELNET входит группа CERT, которая предоставляет соответствующие услуги структурам публичного сектора и сферы образования. В 2008 году несколько НИИ и частных ассоциаций, специализирующихся в сфере компьютерной безопасности, совместно разработали и презентовали экспертный доклад, в котором обосновывается необходимость создания государственной стратегии кибербезопасности, и предлагается ряд мер по повышению уровня информационной безопасности страны.

Бразилия. Вопросами ЗКИИ занимаются, в частности: Комитет по вопросам информационной безопасности, в состав которого входят представители всех министерств и ведомств; государственную политику в сфере информационных и коммуникационных технологий (ИКТ) курируют Министерство науки и технологий, Министерство связи и бразильский Сетевой информационный центр. Бразилия имеет сложную и запутанную систему институтов, участвующих в разработке политики информационной безопасности. Вопросы информационной безопасности входят в компетенцию Министерства по вопросам безопасности государственных институтов (GSI), которое выступает в роли головной организации, отвечающей за координацию мер информационной безопасности. GSI не занимается вопросами безопасности напрямую, а осуществляет свою деятельность через другие уполномоченные организации. Вопросами дальнейшего развития государственно-частного партнерства занимаются Anatel (федеральный регуляторный орган в сфере телекоммуникаций), Serpro (федеральная служба обработки данных) и CERT.br (компьютерная группа реагирования на чрезвычайные ситуации).

Канада. Канадский центр оперативного реагирования на чрезвычайные происшествия в компьютерных сетях (CCIRC) занимается мониторингом и консультированием по вопросам защиты от киберугроз, а также на государственном уровне координирует меры оперативного реагирования на любые чрезвычайные происшествия, прежде всего на государственных объектах критической инфраструктуры. К мероприятиям по борьбе с кибер-угрозами привлекаются несколько ведомств, в том числе Королевская конная полиция Канады, Агентство безопасности связи и Служба безопасности и разведки Канады. В феврале 2010 года правительство в третий раз за последние десять лет объявило о скором появлении Национальной стратегии кибербезопасности.

В **Эстонии** стратегия кибербезопасности опубликована в 2008 году. Этот документ дает описание нынешнего состояния кибербезопасности в государстве и определяет национальную политику в этой сфере. В стране отсутствует единый орган государственной власти, который бы отвечал за ЗКИИ. В этом про-

цессе непосредственно участвуют несколько министерств и их подразделений. Основные задачи в сфере ЗКИИ возложены на Министерство экономики и связи (МЭС/MEAC), которому принадлежит ведущая роль в обеспечении информационной безопасности. В подчинении министерства находятся два органа центральной исполнительной власти, занимающихся реализацией государственной политики компьютерной безопасности. Это Департамент государственных информационных систем (RISO), который выступает в качестве головной организации, осуществляющей общую координацию деятельности в сфере ИКТ, а также Центр информатики Эстонии (RIA), который занимается разработкой и управлением систем передачи данных в интересах государственных организаций, отвечает за техническую безопасность государственных объектов критической информационной инфраструктуры (КИИ), а также следит за общим состоянием безопасности сетей. В составе этого Центра функционирует и Эстонская группа оперативного реагирования на чрезвычайные происшествия в компьютерных сетях (CERT). Сферу почтовых услуг, а также рынок услуг электронной связи координирует Национальный совет по связи. Органы, занимающиеся вопросами ЗКИИ, состоят и в структуре Министерства внутренних дел и Министерства обороны. Оба эти министерства отвечают за внутреннюю безопасность и кризисное управление. В сфере государственно-частного партнерства создан проект «Компьютерная безопасность 2009», который направлен на укрепление информационной безопасности.

В **Финляндии** кибербезопасность рассматривается как проблема безопасности данных, а также как экономическое условие, тесно связанное с развитием финского информационного общества. Вопросами ЗКИИ в основном занимаются три государственных органа: Служба регулирования связи (FICORA) в структуре Министерства транспорта и связи, которая способствует развитию информационного общества и занимается регулированием технических вопросов и стандартизацией; Национальное агентство чрезвычайных ситуаций (NESA), которое занимается оценкой и анализом угроз и рисков безопасности КИИ, а также Главное управление безопасности данных при Государственной администрации (VAHTI), которое разрабатывает руководящие принципы и практические руководства по обеспечению безопасности IT-систем. Кроме того, в сфере ЗКИИ созданы три государственно-частных партнерства. Это Национальный совет по чрезвычайным ситуациям (NESC), Консультативный совет по вопросам информационного общества и Центр по вопросам развития информационного общества Финляндии (TIEKE).

Франция. Вся ответственность за организацию мер ЗКИ возложена на Генеральный секретариат национальной обороны (SGDN) в структуре Администрации премьер-министра. Во Франции кибербезопасность расценивается одновременно как вопрос высокотехнологичной преступности и как проблема, препятствующая нормальному развитию информационного общества. За расследования преступлений в этой сфере отвечают Центральный офис борьбы с преступностью в области технологий связи и информации (OCLCTIC), созданный в мае 2000 года, и отдел экономических и финансовых расследований Главного управления судебной полиции. В июле 2009 года в структуре Министерства обороны было создано Национальное агентство безопасности информационных систем (Anssi), на которого возложены задачи по ЗКИИ и обеспечению кибербезопасности. Кроме того, функционирует и Межведомствен-

ная комиссия по безопасности информационных систем (CISSY). В сфере государственно-частного партнерства создан Стратегический консультативный совет по информационным технологиям (CSTI), который ставит своей целью объединение усилий государственных должностных лиц, бизнеса и топ-менеджеров предприятий, а также представителей научного сообщества.

В **Германии** принята Национальная стратегия безопасности критической инфраструктуры (БКИ). Этот документ определяет цели и задачи правительства в этой сфере, которые, в свою очередь, отражены в Государственной программе безопасности информационной инфраструктуры (NPSI). Ведущая роль в решении вопросов кибербезопасности отводится Федеральному агентству информационной безопасности (BSI), которое входит в структуру Министерства внутренних дел. Совместно с Федеральным агентством гражданской обороны и чрезвычайных ситуаций (BBK), Федеральным агентством криминальной полиции (BKA), Федеральной полицией (BPOL) и Службой технической поддержки федеральных институтов, агентство BSI осуществляет оценку и анализ угроз, формирует концепции защиты. Для координации действий в рамках Министерства и с подведомственными учреждениями создана рабочая группа по ЗКИ (AG KRITIS). Деятельность по разработке стратегии и ее реализации также координируется с другими федеральными министерствами, в частности, Министерством экономики и технологий, Администрацией федерального канцлера, Федеральным министерством юстиции, Федеральным министерством иностранных дел, Федеральным министерством обороны и другими уполномоченными учреждениями, в частности, Федеральным агентством электронных сетей. Кроме того, проводятся консультации со стратегическими партнерами из частного сектора.

Венгрия. В 2006 году правительство страны было реорганизовано. Среди наиболее важных изменений, непосредственно касающихся ЗКИИ и развития информационного общества, следует упомянуть слияние Министерства информатики и связи, которому принадлежала ведущая роль в вопросах ИКТ, с Министерством экономики и транспорта и Администрацией премьер-министра. В настоящее время основные функции в сфере ЗКИИ распределены по различным министерствам. Как уполномоченный орган по вопросам функционирования и развития промышленной инфраструктуры, в том числе информационной, Министерство экономики и транспорта координирует различные программы в сфере ЗКИ и ЗКИИ. При содействии Центра электронного правительства Администрация премьер-министра координирует деятельность электронного правительства и другие вопросы ЗКИИ. Министерство обороны отвечает за национальную безопасность, в том числе безопасность информационных сетей, а также за охрану государственных секретов и государственной информации. В функции и обязанности Министерства юстиции и правоохранительной деятельности входят профилактика преступности и защита информации. Кроме того, это министерство контролирует деятельность Главного управления государственных электронных услуг, которое координирует все вопросы, связанные с предоставлением услуг электронного правительства и управлением электронными записями и документацией. Государственное управление по вопросам связи (NCA) является независимым регуляторным органом в сфере коммуникаций. Этот орган обеспечивает развитие рынка услуг связи с тем, чтобы любой гражданин имел доступ к качественным и при

этом недорогим услугам связи. Он также контролирует деятельность Государственной службы уведомления (NAS) о чрезвычайных происшествиях в почтовой и коммуникационной сферах. Поскольку вопросы информационной безопасности и ЗКИИ затрагивают сферу компетенции сразу нескольких государственных ведомств, для решения этих задач в Венгрии создан ряд межведомственных органов. Кроме того, важная роль в ЗКИИ принадлежит Фонду государственно-частного партнерства им. Теодора Пушкаша, так как в его структуре действует национальная группа оперативного реагирования на чрезвычайные происшествия в компьютерных сетях (CERT-Hungary).

Индия. На вершине государственной системы информационной безопасности находится Национальный информационный совет (NIB) численностью 21 человек. Этот орган работает в тесном взаимодействии с Государственной научно-технической организацией и Государственным координационным центром информационной безопасности (NISCC), который входит в структуру Секретариата Совета национальной безопасности (NSCS). NISCC занимается вопросами оперативного реагирования на чрезвычайные происшествия в компьютерных сетях, научных разработок, кодированной защиты каналов передачи данных, законодательного регулирования, пресечения и раннего оповещения об атаках, подготовки/обучения и международного сотрудничества. NIB поручил NSCS осуществлять координацию деятельности по обеспечению кибербезопасности в масштабах страны. Деятельность Национального совета осуществляется через отраслевые управления кибербезопасности. На следующей ступени системы после NIB находится Центр защиты информационной инфраструктуры (IIPC), за ним – отделения кибер-полиции штатов, затем индийская группа оперативного реагирования на чрезвычайные происшествия в компьютерных сетях (CERT-In) и, наконец, управления кибербезопасности штатов и отраслей. На этом же уровне находятся и специальные органы различных министерств, как, например, Отдел развития и пропаганды при Министерстве связи и информационных технологий (МОС). В рамках государственно-частного партнерства создан Форум кибербезопасности *Индия-США*, задачей которого является обсуждение и расширение двухстороннего сотрудничества в сфере высоких технологий.

В **Италии** головными организациями по вопросам ЗКИИ выступают Министерство внутренних дел (полиция почты и связи) и Министерство инноваций и технологий. Полицейская служба почтовой связи курирует работу центров оперативного реагирования на компьютерные преступления как на национальном, так и региональном уровнях. Министерство связи также участвует в различных видах деятельности по укреплению безопасности информации и сетей связи. В целях совершенствования ЗКИИ на всех уровнях государственные ведомства также тесно сотрудничают с частным сектором. Крупнейшим проектом государственно-частного партнерства в сфере ЗКИ стало создание Ассоциации итальянских экспертов по вопросам критической инфраструктуры (AIIC), которая объединила специалистов-практиков как из государственных организаций, так и частного сектора.

В **Японии** главным действующим лицом в области ЗКИИ и информационной безопасности в целом является Секретариат Кабинета министров. В его структуре функционирует Совет по вопросам стратегии развития информационных

технологий, в состав которого входят 20 авторитетных экспертов. В 2005 году в структуре Секретариата Кабинета министров были созданы Совет по вопросам политики информационной безопасности (ISPC) и Национальный Центр информационной безопасности (NISC), которым сегодня принадлежит ведущая роль в вопросах национальной политики в области ЗКИИ. ISPC играет главную роль в разработке и модернизации стратегий и политики безопасности. Он возглавляется главой Секретариата Кабмина и входит в состав стратегического IT штаба, куда, в сою очередь, входят представители различных министерств и специалисты частных компаний. NISC является центральным органом исполнительной власти по вопросам IT безопасности. Секретариат Кабинета министров действует при поддержке Министерства экономики, торговли и промышленности (METI), Национального полицейского агентства (NPA/НПА), а также Министерства внутренних дел и коммуникаций. METI занимается планированием и реализацией информационной политики под руководством стратегического IT штаба, а также вопросами электронной торговли, электронного правительства, защиты данных, исследований и разработок в сфере информационных технологий. NPA поддерживает компьютерную и сетевую безопасность и расследует киберпреступления, для чего в его составе действует Управление высокотехнологичной преступности (HTCTD), которое занимается предотвращением и недопущением роста крупномасштабных компьютерных инцидентов, а также имеет полномочия по аресту киберпреступников. Одно из его подразделений состоит из мобильных групп технической поддержки, которые размещены по всей Японии и подчинены Центру киберкомандования. MIC отвечает за создание национальной инфраструктуры и ежегодно публикует Белую книгу по вопросам информатизации и связи в Японии. В рамках государственно-частного партнерства действует Центр средств защиты, технической эксплуатации, анализа и реагирования (CEPTOAR), который ставит своей целью улучшение информационного обмена между государством и частным сектором.

В **Республике Корея** вопросами ЗКИИ занимаются все государственные организации и их дочерние структуры. Деятельность всех этих министерств и ведомств координирует Национальный центр кибербезопасности (NCSC), который работает под эгидой Национальной службы разведки (NIS). Кроме того, NCSC служит платформой, которая объединяет в борьбе с киберугрозами участников частного, публичного и военного секторов и является центральным органом исполнительной власти в вопросах выявления и предотвращения кибератак, а также оперативного реагирования на кибер-угрозы. Координацией деятельности по расследованию и профилактике киберпреступлений занимается специализированный следственный орган при Генеральной прокуратуре Японии. НИИ электроники и телекоммуникаций (ETRI) играет ведущую роль в разработке соответствующих технологий и обеспечении мероприятий по ЗКИИ. Министерство государственного управления и безопасности (MOPAS), Корейская комиссия связи, Министерство знаний и экономики Кореи, Корейский центр интернет-безопасности (KrCERT/CC) в составе Корейского агентства информационной безопасности (KISA) содействуют формированию культуры безопасного Интернета и телекоммуникационных сетей и несут общую ответственность за мероприятия в сфере ЗКИИ. В состав KISA входит Отдел защиты информационной инфраструктуры, состоящий из группы планирова-

ния мероприятий ЗКИИ, группы управления безопасностью критической инфраструктуры и главной группы Корейской службы сертификации. Национальный альянс информационной безопасности (NISA), куда входят представители 22-х государственных организаций, руководители служб информационной безопасности 17-ти предприятий (государственные компании и операторы информационных сетей), а также специалисты из промышленных и научных кругов, является государственно-частным партнерством, которое направлено на повышение информационной безопасности путем содействия информационным обменам.

Малайзия. Вопросы безопасности сетей в государственном секторе курирует Управление модернизации и планового менеджмента (MAMPU), куда входит отдел безопасности ИКТ и государственная компьютерная группа экстренного реагирования. На базе Управления действует государственный командный центр информационной безопасности, который занимается мониторингом киберугроз. Широкий круг обязанностей, касающихся национальной политики в области ИКТ, ЗКИИ и кибербезопасности выполняет Министерство науки, технологий и инноваций (MOSTI). Полицейское подразделение по борьбе с киберпреступностью отвечает за расследование и предотвращение коммерческой киберпреступности, а мероприятиями по ЗКИ занимается Министерство энергетики, водного хозяйства и связи (MEWC). Комиссия по связи и мультимедиа (MCMC) выполняет координирующую функцию и обеспечивает информационную безопасность, целостность и надежность малазийских информационных сетей.

В **Нидерландах** ответственность за реализацию политики ЗКИИ возложена на ряд государственных ведомств, но координирующие функции исполняет Министерство внутренних дел и по делам Королевства. Кроме того, это министерство курирует деятельность других уполномоченных ведомств, а также вопросы международной политики и кризисного менеджмента, которыми занимается созданный в структуре министерства Национальный кризисный центр. В мероприятиях по защите информационной безопасности также принимает участие Служба общей разведки и безопасности (AIVD).

Новая Зеландия. Центральным органом исполнительной власти по вопросам кибербезопасности является Центр защиты критической инфраструктуры (CCIP) при Агентстве безопасности государственных сетей. Центр работает в тесном сотрудничестве с организациями государственной критической инфраструктуры (ГКИ/CNI), промышленным сообществом и правительством по совершенствованию методов ЗКИИ и обеспечения компьютерной безопасности. CCIP стремится стать надежным и авторитетным источником информации по вопросам безопасности ГКИ. Он работает в режиме 24/7 и обеспечивает постоянное наблюдение за состоянием сетей и оповещение об угрозах, а также проводит расследование и анализ чрезвычайных происшествий в сетях. Ведущая роль в разработке политики безопасности Новой Зеландии, в том числе кибербезопасности, принадлежит Секретариату внутренних и иностранных дел (DESS), который возглавляет премьер-министр. Агентство безопасности государственных сетей (GCSB) дает консультации и оказывает помощь министерствам и ведомствам в вопросах, касающихся защиты систем обработки информации, и подчиняется непосредственно премьер-министру.

Норвегия. Управление гражданской обороны и кризисного планирования (DSB) выступает в качестве головной организации в области кризисного планирования в гражданской сфере, и ему же принадлежит ведущая роль в координации деятельности по ЗКИ/ЗКИИ. Управление находится в подчинении Министерства юстиции и полиции. Общие полномочия по безопасности информации и сетей связи сосредоточены в Министерстве государственного управления и реформ. Министерство обороны отвечает за безопасность военных компьютерных сетей. Министерство транспорта и связи отвечает за сектор связи, в том числе и за все аспекты безопасности информационных сетей. Служба национальной безопасности Норвегии (NSA) координирует меры по обеспечению безопасности компьютерных сетей. Государственный координационный совет по вопросам информационной безопасности (KIS) не наделен полномочиями по принятию решений, но служит платформой для обсуждения и консультирования министерств и ведомств по вопросам, касающимся безопасности ИК сетей, ЗКИ и ЗКИИ. В его состав входят представители шести министерств, аппарата премьер-министра и десяти различных управлений.

Польша. За информационную инфраструктуру и ее безопасность отвечают два ведомства. Это Министерство науки и высшего образования и Министерство внутренних дел и администрации. Главным субъектом и единственным координатором научно-технической политики государства выступает Министерство науки и высшего образования, которое участвует в разработке всех стратегий, касающихся информационной инфраструктуры и ее безопасности. Это ведомство разрабатывает стратегические рекомендации для всех остальных министерств и ведомств и обеспечивает совместимость государственных компьютерных сетей. Министерство внутренних дел и администрации отвечает за государственную компьютерную инфраструктуру, государственную систему телекоммуникаций и систему управления государственными информационными сетями.

В **России** головными организациями в сфере информационной безопасности являются Совет безопасности, Федеральная служба безопасности (ФСБ), Федеральная служба охраны, Федеральная служба технического и экспортного контроля и Министерство информационных технологий и связи. Совет безопасности определяет национальные интересы России в информационной сфере, определяет объекты и другие ресурсы, которые должны быть защищены, а также координирует разработку стратегии информационной безопасности. ФСБ отвечает за безопасность Российской Федерации и ЗКИИ. В составе Службы контрразведки ФСБ функционирует Управление компьютерной и информационной безопасности. ФСБ занимается планированием и реализацией государственной научно-технической политики в сфере информационной безопасности, обеспечивает криптографическую и инженерно-техническую защиту ИК сетей, защищает государственные секреты и все виды связи. Федеральная служба охраны имеет в своем составе Службу специальной связи и информации, которая взяла на себя часть функций, ранее входивших в компетенцию Федерального агентства правительственной связи и информации (ФАПСИ) до его упразднения в 2003 году. Остальные функции ФАПСИ были распределены между ФСБ, Службой охраны и Генеральным штабом вооруженных сил. Служба технического и экспортного контроля подчинена Министерству обороны. В сферу ее компетенции входят информационная безопасность

систем ИКТ, противодействие техническому шпионажу иностранных государств и защита секретной информации. Министерство информационных технологий и связи реализует государственную политику и осуществляет надзор в секторе связи.

Сингапур. Управление безопасности информационных сетей и связи (SITSA) в составе Департамента внутренней безопасности при Министерстве внутренних дел (МВД) выполняет функции по защите компьютерных сетей от угроз национальной безопасности, в том числе кибертерроризма и кибершпионажа, а также отвечает за разработку и реализацию соответствующих мер безопасности на национальном уровне. SITSA проводит мероприятия по ЗКИИ и совершенствованию возможностей экстренного реагирования. За безопасность отраслевых сетей отвечают регуляторные органы соответствующих ведомств. При этом функция общего руководства этой деятельностью возложена на SITSA. Ответственность за государственные информационные сети и связь возложена на Управление развития ИКТ сетей (IDA) в составе Главного государственного информационного управления (GCIO). Формированием государственной политики кибербезопасности и разработкой соответствующих национальных стратегий занимается Государственный комитет информационной безопасности (NISC), где IDA выполняет роль секретариата.

В **Испании** различные аспекты политики ЗКИ/ЗКИИ в основном находятся в компетенции Министерства промышленности, туризма и торговли, Министерства государственного управления и Министерства внутренних дел. Под управлением Министерства промышленности, туризма и торговли функционируют Государственный секретариат по делам туризма и торговли и Государственный секретариат по телекоммуникациям и вопросам информационного общества. Последний руководит деятельностью Главного управления по телекоммуникациям и информационным технологиям (DGTTI) и Главного управления по вопросам развития информационного общества (DGDSI). Министерство государственного управления курирует три крупных национальных проекта в сфере развития и безопасности информационных и телекоммуникационных сетей: Совет электронного правительства, Технический комитет Совета электронного правительства и проект Technimap. В задачи Совета электронного правительства входят подготовка, разработка, развитие и применение государственной политики и стратегий в компьютерной сфере, а также, совместно с Национальным центром криптологической защиты при Национальном разведывательном Центре, разработка мер безопасности информации и телекоммуникаций и соответствующих сетей. Технический комитет по вопросам безопасности информационных систем и обработки персональных данных (SSITAD) отвечает за борьбу с кибер-угрозами и обеспечение деятельности Совета электронного правительства. Technimap представляет собой национальный форум по вопросам развития и безопасности информации и телекоммуникационных сетей, в котором принимают участие специалисты различных государственных ведомств, крупных компаний и других заинтересованных структур. Борьбой с киберпреступностью под общим руководством Министерства внутренних дел занимаются Национальная полиция и Гражданская гвардия. Для этого в структуре Национальной полиции существует Управление компьютерной преступности, а в Гражданской гвардии действует Департамент по противодействию преступности в сфере высоких тех-

нологий. Национальный департамент полиции и Генеральный департамент судебной полиции имеют службу экстренного реагирования на преступления в компьютерных сетях. Руководством, координацией и надзором в сфере ЗКИ занимается Национальный центр защиты критической инфраструктуры (CNPIC). Кроме того, в этой сфере созданы и два государственно-частных партнерства: это Аналитический центр по вопросам информационного общества и телекоммуникаций (ENTER) и Испанская ассоциация электронной, компьютерной и телекоммуникационной промышленности (AETIC).

Швеция. В мероприятиях ЗКИ/ЗКИИ участвуют множество организаций. В 2009 году Шведскому агентству гражданской обороны (MSB) при Министерстве обороны было поручено до января 2010 года представить предложения по предотвращению и устранению последствий преступлений в компьютерных сетях. В составе Агентства было решено создать Национальный оперативный координационный центр кибербезопасности, который будет координировать совместные мероприятия на межведомственном уровне и выступать в роли центрального элемента системы кризисного менеджмента. Важная роль в этом процессе принадлежит и Агентству по чрезвычайным ситуациям (SEMA) при Министерстве обороны. Кроме того, существует Группа по совместным операциям в сфере информационной безопасности (SAMFI) под руководством MSB, куда входят представители шведских Вооруженных сил, Национальной службы радиотехнической обороны (FRA), Национального агентства почты и телекоммуникаций (PTS) и Национального Департамента полиции. В рамках межведомственного сотрудничества на уровне Кабинета министров проводится работа по реализации рекомендаций агентства SEMA и модернизации национальной системы ЗКИИ. На уровне государственно-частного партнерства осуществляются такие инициативы, как проект агентства SEMA по расширению взаимодействия между государственным и частным секторами в этой сфере, проект «Делегация промышленной безопасности» (NSD) и проект «Шведское общество обработки информации» (DFS).

Швейцария. Вопросами ЗКИ/ЗКИИ занимаются целый ряд различных организационных подразделений. Одной из головных организаций в этой сфере выступает Федеральное стратегическое подразделение по информационным технологиям (FSUIT). Являясь частью Федерального департамента финансов, оно разрабатывает инструкции, методологии и процедуры в сфере информационной безопасности, курирует деятельность Специальной рабочей группы по информационному обеспечению (SONIA) и Информационно-аналитического центра по вопросам информационного обеспечения (MELANI), который осуществляет поддержку деятельности Координационной группы по противодействию киберпреступности (KOBIK). Оба эти подразделения находятся в ведомстве Федерального управления полиции (FEDPOL). Федеральное управление информационных технологий, сетей и телекоммуникаций (FOITT) также является частью Федерального департамента финансов и отвечает за безопасность и экстренную готовность федеральных IT-систем на оперативном уровне. В сфере информационной безопасности также действуют Управление информационной и телекоммуникационной инфраструктуры при Федеральном ведомстве экономических ресурсов, Федеральное управление гражданской обороны (FOCP, отвечает за ЗКИ) и государственная группа экстренного реагирования на чрезвычайные происшествия в информационных сетях. За

безопасность военных компьютерных сетей отвечает Служба поддержки командования Вооружённых сил (Führungsunterstützungsbasis – FUB). Государственно-частное партнерство играет огромную роль в реализации политики ЗКИИ Швейцарии.

Великобритания. Стратегия кибербезопасности 2009 года подчеркивает необходимость комплексного подхода к обеспечению кибербезопасности, в реализации которого должны участвовать правительство, организации всех отраслей промышленности, а также организации гражданского общества и международные партнеры. Стратегия предусматривает создание двух новых организаций (обе начали свою деятельность в марте 2010 года). Во-первых, это Управление кибербезопасности (OCS) в структуре Кабинета министров, которое обеспечивает стратегическое руководство и согласованность действий на межведомственном уровне. Оно же будет заниматься координацией действий по предупреждению киберпреступности. При этом будут использоваться уже существующие возможности, находящиеся в распоряжении Министерства обороны, разведывательных служб и полиции (отдел Лондонской полиции по борьбе с электронной преступностью, Центр по противодействию детской эксплуатации и защите Интернет-сетей, а также Агентство по вопросам особо опасной и организованной преступности, Soca). Во-вторых, это Оперативный центр кибербезопасности (CSOC) на базе штаба правительственной связи в г. Челтенхем. Этот новый центр возьмет на себя уже существующие функции разных ведомств по мониторингу состояния киберпространства и координации мер экстренного реагирования. Кроме того, он будет заниматься анализом угроз для компьютерных сетей Великобритании и их пользователей, а также разрабатывать соответствующие рекомендации и информационные пособия. В составе Центра по защите национальной инфраструктуры (CPNI) действует служба «скорой компьютерной помощи» (CERT service).

Приложение 2

МЕРЫ ПРОТИВОДЕЙСТВИЯ МЕЖДУНАРОДНОГО И РЕГИОНАЛЬНОГО УРОВНЕЙ [46]

Совет Европы

Европейская Конвенция по борьбе с киберпреступностью (CETS 185), разработанная в рамках Совета Европы при участии представителей Канады, Японии, ЮАР и США, была открыта для подписания 23 ноября 2001 года в Будапеште и вступила в силу 1 июля 2004 года. Эта Конвенция открыта для присоединения к ней любой страны и является единственным юридически обязательным международным договором по данному вопросу, принятым на сегодняшний день. Протокол о преступлениях на почве ксенофобии и расизма, совершенных посредством компьютерных сетей (CETS 189), был открыт для подписания в январе 2003 года и вступил в силу в марте 2006 года.

Конвенция обязывает подписавшиеся страны создать нормативно-правовую базу, необходимую для эффективного решения проблем киберпреступности, и взять на себя обязательства по оказанию помощи другим подписавшимся странам в расследовании и судебном преследовании киберпреступников. Европейская Конвенция является одним из первых международных документов, содержащих классификацию киберпреступлений. В частности, введены определения несанкционированного доступа в ИТ-среду, незаконного перехвата ИТ-ресурсов, вмешательства в компьютерную систему и информацию, содержащуюся на носителях, неправомерного использования оборудования; компьютерного мошенничества. Сфера ее действия также распространяется на преступления, связанные с детской порнографией и нарушением авторских и смежных прав. Конвенция определяет инструменты для эффективного расследования компьютерных преступлений и борьбы с ними. Ее действие распространяется на любые преступления, совершенные с применением компьютерных систем, а также любые доказательства, собранные при помощи электронных средств.

На сегодняшний день Конвенцию ратифицировали двадцать восемь стран (страны ЕС и США) и подписали сорок шесть стран (страны ЕС, Канада, Япония, Южная Африка, все страны-члены НАТО). Пяти странам (Чили, Коста-Рика, Доминиканская Республика, Мексика, Филиппины) предложено присоединиться к Конвенции. Две большие страны, а именно Китай и Россия Конвенцию подписывать отказались. Европейская конвенция используется в качестве руководства, справочного пособия либо стандартного или типового закона в более чем 100 странах мира. Кроме того, Конвенция поддерживается другими организациями, которые ссылаются на нее в своих решениях. Это Европейский союз, Организация Американских государств (ОАГ), Организация экономического сотрудниче-

[46] Материалы для данного приложения были любезно предоставлены господином Фредом Шрайером.

ства и развития (ОЭСР), Организация Азиатско-Тихоокеанского экономического сотрудничества, Интерпол, а также структуры частного сектора.

Несмотря на широкое международное признание Конвенции, некоторые из стран утверждают, что она предусматривает недостаточно мер для противодействия преступлениям, которые могут поставить под угрозу интересы национальной безопасности. Во-первых, Конвенция классифицирует атаки на IT-сети как уголовное преступление против частной и государственной собственности, а не как угрозу национальной безопасности. Во-вторых, Конвенция не делает различий между атаками на обычные компьютерные сети и объекты критической информационной инфраструктуры, как и различий между крупномасштабными и локальными атаками.

Тем не менее, Конвенция представляет собой стандартную, но очень важную часть международного законодательства. В ней содержится оптимальный комплекс юридических и технических норм, которые могут послужить основой для разработки дополнительных соглашений по расширению международного сотрудничества в этой сфере. Поскольку киберпреступность, кибертерроризм и кибервойна имеют много общих признаков, предусмотренная Конвенцией ответственность за любые кибератаки, независимо от их мотивов, предполагает, что подписавшие ее страны должны по требованию уполномоченных органов задерживать и передавать в руки правосудия всех международных киберпреступников, независимо от того, рассматриваются ли они в собственной стране как преступники, террористы или даже как патриоты, действия которых достойны похвалы и уважения.

Европейский Союз

ЕС является ключевым субъектом международной деятельности в сфере обеспечения информационной безопасности. При этом ЕС уделяет основное внимание таким вопросам, как ЗКИИ, формирование информационного общества и защита информации. ЕС приступил к реализации ряда проектов и научно-исследовательских программ по изучению различных аспектов информационной революции и ее влияния на образование, бизнес, здоровье и связь.

Коммюнике о *Защите критической инфраструктуры в рамках борьбы с терроризмом*, принятое Комиссией европейских сообществ (Комиссия ЕС) 20 октября 2004 года, дает определение критической инфраструктуры (КИ), определяет объекты КИ и устанавливает критерии для определения объектов КИ, которые могут появиться в будущем. В ноябре 2005 Комиссия ЕС приняла *«Зеленую книгу» по европейской программе ЗКИ*, где определены направления деятельности ЕС в сфере ЗКИИ. В 2008 году Комиссия ЕС приступила к реализации проекта по выработке общей стратегии ЗКИИ.

Среди *других проектов и стратегий Комиссии ЕС* следует отметить:

- проводимые по заказу Комиссии исследования по проблемам доступности и надежности инфраструктур электронной связи (ARECI);
- проект «Информационная сеть оповещения об угрозах для критической инфраструктуры» (CIWIN);
- Европейское агентство сетевой и информационной безопасности (European Network and Information Security Agency – ENISA) было создано в марте 2004 года и приступило к работе в сентябре 2005 года на острове

Крит. ENISA ставит своей целью достижение высокого уровня безопасности сетей электронной связи в рамках всего Европейского союза;

- TESTA: Трансъевропейская межправительственная служба телеметрии (Trans-European Service for Telemetrics between Administrations). Это сеть межправительственной связи, действующая только в рамках Евросоюза. Она не соединена с Интернетом и позволяет должностным лицам различных ведомств общаться на трансъевропейском уровне, не опасаясь утечки или повреждения информации.

Научно-исследовательские проекты ЕС в сфере информационной безопасности:

- «Технологии информационного общества». Проекты FP6 и FP7;
- Европейская научно-исследовательская программа по проблемам безопасности (ESRP);
- Координационный проект научных исследований по проблемам критической информационной инфраструктуры (CI2RCO);
- Проект «Архитектура сервисов и ПО, инфраструктуры и проектирование».

Нормативно-правовая база ЕС по вопросам информационной безопасности:

- Директива о защите данных (1995 г.);
- Директива об электронной подписи (1999 г.);
- Директива о защите конфиденциальности в сфере электронной связи (2002 г.);
- Рамочная директива (2002 г.);
- Рамочное решение Совета об атаках на информационные системы (2005 г.);
- Директива о хранении данных (2006 г.).

Форум команд экстренного реагирования и безопасности (FIRST)

Форум основан в 1990 году и является единственным в мире международным форумом для специалистов по экстренному реагированию на инциденты в сфере информационной безопасности. Эта организация является признанным мировым лидером в сфере экстренного реагирования на инциденты в сетях и объединяет группы оперативного реагирования, работающие на самых разных уровнях, от правительств и корпораций до образовательных учреждений. Деятельность Форума направлена на укрепление и координацию сотрудничества по предотвращению инцидентов, развитие возможностей в сфере быстрого реагирования, а также содействие информационным обменам между членами организации и обществом в целом.

Большая восьмерка (Group of Eight – G8)

С 1995 года Большая восьмерка принимает все более активное участие в решении вопросов, связанных с киберпреступностью, информационным обществом, ЗКИ и ЗКИИ. На саммите в Галифаксе в 1995 году группе старших экспертов было поручено проанализировать и оценить существующие международные соглашения и механизмы борьбы с организованной преступностью. По результатам проведенного анализа Группа старших экспертов Большой восьмерки разработала сорок оперативных рекомендаций, которые были утверждены на сам-

мите Большой восьмерки в Лионе в 1996 году. С тех пор эта Лионская группа превратилась в постоянный многофункциональный орган, в состав которого вошли целый ряд специализированных рабочих подгрупп. С октября 2001 года заседания Лионской группы проводятся совместно с Римской группой по борьбе с терроризмом.

Еще одним важным этапом деятельности Большой восьмерки в области ЗКИ/ЗКИИ стал 2000 год, когда в Париже с участием представителей правительств и промышленных кругов состоялась Конференция стран Большой восьмерки, посвященная развитию государственно-частного партнерства в сфере безопасности и повышения доверия в киберпространстве. Конференция была организована с целью обсуждения общих проблем и поиска решений по противодействию высокотехнологичной преступности и использованию Интернета в преступных целях. Государства Большой восьмерки договорились о выработке четких и прозрачных принципов борьбы с киберпреступностью. Утвержденные ими принципы направлены на создание новой «культуры безопасности», активизацию международного сотрудничества, а также распространение передового опыта в сфере мониторинга и оповещения об угрозах в компьютерных сетях. Они предложили провести совместные учения, которые должны выявить уровень готовности служб экстренного реагирования на чрезвычайные происшествия в сетях, а также донести информацию об угрозах до правительств других стран и побудить их к принятию соответствующих мер противодействия, которые принимаются на уровне Большой восьмерки. Эти одиннадцать руководящих принципов помогут государствам построить эффективную национальную политику в сфере защиты ключевой информационной инфраструктуры (ЗКИИ).

Основные элементы этих принципов ЗКИИ нашли свое отражение в Резолюции ООН № 58/199 «О создании глобальной культуры кибербезопасности и защите критической информационной инфраструктуры», которая была принята на 78-м заседании Генеральной Ассамблеей ООН в январе 2004 года.

Организация Североатлантического договора (НАТО)

НАТО разработало и запустило собственную программу кибер-обороны в 2002 году после серии сетевых инцидентов, которые произошли во время операции на Балканах в конце 1990-х годов. Руководство НАТО учло эти уроки, и во время Пражского саммита 2002 года лидеры стран НАТО договорились о разработке Программы кибернетической обороны и создании собственной группы экстренного реагирования на инциденты в информационных сетях (NCIRC). Координационный центр NCIRC был создан при штаб-квартире НАТО в Брюсселе, а при штабе Союзного командования операций НАТО (г. Монс, Бельгия) был организован Технический центр NCIRC. С созданием этих структур альянс получил возможности для решения ряда важнейших задач – от обнаружения и нейтрализации вредоносного ПО и несанкционированных вторжений в сети НАТО до управления криптографической защитой сетей, имеющих выход в Интернет.

Кроме того, эксперты НАТО обеспечивают техническую поддержку при возникновении угрозы безопасности компьютерный сетей, а также разрабатывают режимы обеспечения безопасности и методологии расследований компьютерных преступлений. Помимо созданного в Таллинне Объединенного центра обмена передовым опытом в сфере компьютерной обороны НАТО (Cooperative Cyber Defense Centre of Excellence/CCDCOE), альянс учредил и специальный орган по

управлению мероприятиями кибер-обороны (CDMA), который действует с апреля 2008 года. На него возложены функции по организации и координации «оперативных и эффективных мер кибер-обороны» в случае атак на компьютерные сети альянса. На саммите НАТО в Страсбурге/Келе в апреле 2009 года страны НАТО обязались ускорить приобретение современных средств кибероборонs, сделать киберзащиту неотъемлемой частью учений НАТО, а также укреплять связи между НАТО и странами-партнерами в сфере защиты от кибератак. Совсем недавно руководство НАТО подтвердило свою готовность оказать странам альянса всемерную помощь в создании групп экстренного реагирования на кибер-угрозы.

ЗКИ остается одним из ключевых направлений деятельности НАТО в сфере планирования гражданской обороны. Необходимость мер по ЗКИ несколько раз подчеркивается в документе о принципах планирования гражданской обороны, разработанных для соответствующих ведомств стран альянса. Кроме того, ряд мероприятий ЗКИ предусмотрены и в новой редакции Плана действий по планированию гражданской обороны, который призван повысить уровень готовности гражданских служб к чрезвычайным ситуациям, связанным с применением химического, биологического и ядерного оружия. Главный Комитет НАТО по планированию гражданской обороны и восемь его отделов и комитетов продолжают изучение функциональных аспектов ЗКИ. По результатам этой работы разрабатываются рекомендации по всем видам планирования, которыми занимаются соответствующие отделы и комитеты.

В *Специальном докладе*, *представленном на Парламентской ассамблее НАТО в 2007 году*, и в последующих отчетах по вопросам киберзащиты НАТО (173 DSCFC 09 E bis) определены общие принципы стратегий в области ЗКИ стран НАТО и альянса в целом. Они определяют различные нормы, подчеркивают их сходства и различия, а также определяют субъектов ЗКИ вместе с их функциями и обязанностями в сфере разработки и реализации отраслевых стратегий ЗКИИ, в том числе в сфере энергетики, гражданской авиации и безопасности морских портов.

Организация экономического сотрудничества и развития (ОЭСР)

ОЭСР имеет богатый опыт в разработке стратегических рекомендаций по вопросам безопасности компьютерных систем и сетей, в том числе в сфере ЗКИИ. Большое внимание уделяется и вопросам борьбы с киберпреступностью, в частности, связанной с использованием вредоносного программного обеспечения. ОЭСР готовит аналитические отчеты, статистические данные и стратегические рекомендации, на основе которых правительства и структуры частного бизнеса могут разработать эффективные стратегии укрепления собственной информационной безопасности, повысить уровень информированности общества о значении информационной безопасности и способствовать развитию общей культуры безопасности на уровне общества в целом. Все страны ОЭСР согласны с тем, что безопасность и надежность функционирования информационных инфраструктур являются необходимым условием для ведения законной торговли в Интернете, обеспечения безопасности транзакций и защиты персональных данных. Именно поэтому Рабочая группа ОЭСР по информационной безопасности и конфиденциальности (РГИБК/WPISP) активно работает в направлении создания согласованного международного подхода к разработке политики в этой сфере с целью укрепления доверия в IT-сетях. Кроме того, Комитет по информационной,

компьютерной и коммуникационной политике (МККП) проводит анализ общих принципов, лежащих в основе электронной экономики, информационных инфраструктур и информационного общества.

Организация Объединенных Наций (ООН)

Вопросы ЗКИИ осуждаются на уровне ООН с конца 1980-х годов, однако формальные меры начали внедряться только в последнее время. С тех пор был предпринят ряд инициатив по улучшению координации действий. В частности, это проекты некоторых структур ООН, несколько резолюций ООН, а также итоги Всемирных Саммитов ООН по вопросам информационного общества (WSIS).

Исследовательский институт ООН по проблемам разоружения (UNIDIR) организовал серию семинаров по вопросам укрепления международной информационной безопасности в глобальном цифровом пространстве. В свою очередь, Управление ООН по борьбе с наркоманией и преступностью организовывает совместные учения с целью выработки согласованного комплексного подхода к решению проблем киберпреступности.

В декабре 2000 и 2001 годов на 55-й и 56-й сессиях Генеральной Ассамблеи ООН были приняты Резолюции № 55/63 и 56/121 «О борьбе с преступным использованием информационных технологий». В декабре 2002 года на 57-й сессии Генеральной Ассамблеей ООН была принята Резолюция № 57/239 о «Создании глобальной культуры кибербезопасности». В декабре 2003 года на 58-й сессии Генеральной Ассамблеи ООН была принята Резолюция № 58/199 «О создании глобальной культуры кибербезопасности и защите критической информационной инфраструктуры». В приложении к этой Резолюции сформулированы одиннадцать принципов ЗКИИ. В последующие годы Генеральная Ассамблея ООН регулярно принимала Резолюции по «Развитию в области информации и телекоммуникаций в контексте международной безопасности». В 2005 и 2006 годах были приняты еще две Резолюции по итогам очередных Всемирных Саммитов ООН по вопросам информационного общества (WSIS).

Следующим важным шагом стало создание по просьбе Экономического и социального совета ООН Целевой группы ООН по вопросам ИКТ в ноябре 2001 года. Эта группа получила полномочия по мобилизации усилий международного сообщества для реализации положений Декларации «О целях развития тысячелетия» (ЦРТ) в части, касающейся развития информационно-коммуникационных технологий. В апреле 2004 года в штаб-квартире НАТО состоялся семинар на тему «Политика и вопросы безопасности в сфере информационных технологий». В 2005 году Целевая группа опубликовала практическое руководство на тему «Незащищенность информации – пособие по освоению «неисследованных территорий» киберугроз и кибербезопасности», в котором авторы попытались создать общую картину таких новых и серьезных угроз международной безопасности, как киберхулиганство, киберпреступность, кибертерроризм и кибервойна.

В ходе всемирного саммита по вопросам информационного общества лидеры мировых держав назначили Международный союз электросвязи (МСЭ) координатором международной деятельности в области кибербезопасности. Как единственный координатор международной деятельности в сфере укрепления доверия и безопасности при использовании информационно-коммуникационных технологий, МСЭ в мае 2007 года объявил о создании Глобальной программы кибербезопасности (GCA). Эта программа должна выработать комплекс общих

принципов и механизмов для координации и объединения усилий мирового сообщества в деле борьбе с растущими угрозами кибербезопасности. Для реализации программы GCA создана Экспертная группа высокого уровня, в которую вошли более сотни признанных в мире специалистов по кибербезопасности, представляющих правительства, промышленное сообщество, международные организации, исследовательские институты и научные круги. В течение 2007 и 2008 годов МСЭ осуществила большой объем работ по стандартизации архитектур безопасности, методологий кодирования каналов связи и авторизации пользователей сетей и управления безопасностью информационных систем. Кроме того, подготовлена «дорожная карта» стандартов безопасности ИКТ. Она представляет собой электронную базу данных, где содержится информация об уже существующих стандартах безопасности ИКТ, а также о текущих проектах основных организаций, занимающихся разработками международных норм и стандартов.

Группа Всемирного банка

Растущие масштабы компьютерных преступлений и несанкционированных вторжений в электронные сети особенно больно бьют по финансовому сектору. Учитывая постоянно увеличивающиеся объемы хранящейся и передающейся по сети финансовой информации, проблему осложняет то, с какой легкостью преступникам удается проникать в сети и осуществлять там свои вредоносные замыслы. Поэтому Группа Всемирного банка за последние несколько лет предприняла ряд шагов по решению проблем информационной безопасности, особенно в развивающихся странах.

Департамент глобальных информационно-коммуникационных технологий (ДГИКТ) содействует развивающимся странам в получении доступа к ИКТ и обеспечивает деятельность основных департаментов Группы Всемирного банка в вопросах, касающихся исследований, политики, инвестиций и программ в сфере ИКТ.

В 2003 году был издан «Справочник по компьютерной безопасности», где рассматривается передовой опыт и даются рекомендации по обеспечению информационной безопасности, которые могли бы пригодиться всем странам, независимо от уровня их технических возможностей. Эти рекомендации опубликованы на соответствующем веб-сайте и постоянно обновляются по мере появления новых технологий и методик.

В июне 2002 года Всемирный банк опубликовал специальный доклад «*Электронная безопасность: снижение рисков при осуществлении финансовых операций*». Этот документ продолжает серию публикаций, где безопасность электронных сетей в вышеуказанной сфере рассматривается как одно из ключевых условий эффективного функционирования рынка электронных платежей.

В январе и мае 2004 года вышла следующая публикация под названием «Контрольный список технологических рисков» (Technology Risk Checklist), где дается описание тринадцати уровней электронной безопасности, и рассматриваются риски, связанные с работой как аппаратного, так и программного обеспечения сетевой инфраструктуры. Для каждого из этих уровней предусмотрены свои меры по управлению рисками, интеллектуальному централизованному управлению и киберразведке; контролю доступа и авторизации; а также меры межсетевой защиты, активной фильтрация контента; системы обнаружения вторже-

ний, антивирусные системы, средства кодирования и тестирования уязвимости; меры системного администрирования; планы экстренных мероприятий на случай вторжений. В 2005 году вышли в свет еще два документа по вопросам безопасности систем электронных платежей, где рассматривались угрозы, исходящие от бот-сетей и паразитного ПО, а также проблема отмывания денег в киберпространстве.

Всемирная инициатива кибербезопасности Института «Восток-Запад» (WCI)

В 2007 году американская группа «Стратегический диалог» Института «Восток – Запад» (США) во главе с генералом (ныне – в отставке) Джеймсом Джонсом, (бывший Верховный главнокомандующий Объединенных вооруженных сил НАТО в Европе, а ныне советник по национальной безопасности США) провела серию встреч с представителями китайского и российского руководства, где обсуждались возможности выхода из тупика в международном сотрудничестве в сфере кибербезопасности. Активная дискуссия по этому вопросу продолжилась на более высоком уровне в ходе второго раунда переговоров (Track-2). Каждая из трех сторон подтвердила свои опасения в отношении намерений и действий двух других сторон. Но эта дискуссия также выявила и глубокую общую озабоченность США, России и Китая по поводу растущих возможностей негосударственных субъектов, которые способны своими действиями поставить под угрозу стабильность мировой экономики, а сами при этом превращаются в серьезную угрозу для международной безопасности. В результате все три страны пересмотрели свои оценки в вопросах кибербезопасности, а США даже поставили ее на один уровень с проблемой ядерной безопасности.

Сегодня США, Россия и Китай сотрудничают в рамках Инициативы всемирной кибербезопасности, общее руководство которой осуществляет Институт «Восток-Запад». К ним присоединились ведущие деятели Евросоюза и других стран Большой Двадцатки, а также структуры частного бизнеса, профессиональные ассоциации и международные организации.

Консультативную группу WCI возглавил директор Центра киберинноваций «Deloitte» генерал Гарри Рейдуэдж. Эта группа предлагает решение проблемы на двух уровнях: (1) укрепление доверия путем совместного решения конкретных проблем кибербезопасности в сотрудничестве с небольшими группами экспертов из двух или нескольких стран; (2) инициирование общественного процесса, который позволит сделать первые шаги по реализации международной политики безопасности в киберпространстве, как это уже делается по отношению к морскому, воздушному и космическому пространству. Деятельность по этому второму направлению начнется в мае 2010, когда 200 лидеров стран «Кибер-40» (Большая двадцатка и еще 20 крупнейших стран киберпространства) соберутся в Далласе в рамках первого всемирного саммита по вопросам кибербезопасности, который пройдет под эгидой Института «Восток-Запад». Этот форум, который станет первой попыткой создания движения государственно-частного партнерства на таком высоком уровне, будет посвящен вопросам киберзащиты критической инфраструктуры (финансовый сектор, энергетика, телекоммуникации и основные государственные ведомства и службы).

О серии «Горизонт 2015»

Вопросам растущей роли частных военных и охранных предприятий (ЧВОП) посвящено огромное количество материалов и публикаций. В последнее время все больше внимания уделяется вопросу привлечения этих субъектов к процессам реформирования и управления сектором безопасности. Однако пока лишь в очень немногих публикациях рассматривается следующий логичный шаг и анализируется роль частных и других негосударственных субъектов в решении более широкого круга проблем управления безопасностью. В ближайшие годы мы должны будем расширить рамки наших аналитических исследований и вывести их далеко за пределы используемых ныне подходов к реформированию и управлению сектором безопасности. Сегодня пора отказаться от уже устаревшего подхода «целостного государственного управления» (когда та или иная проблема решается не отдельными ведомствами, а на уровне всего правительства), который возник в результате первой волны революции в этой области. Необходимо срочно включиться во второй этап революции. Он требует принятия нового системного подхода, при котором сектор безопасности рассматривается как единый целостный организм, а масштабы решения проблем выходят за рамки существующих государственных структур и охватывают и некоторые частные компании.

Этот проект объединяет заинтересованные государственные и негосударственные структуры в рамках нескольких тематических круглых столов, которые состоятся в течение 2010 года. По результатам каждого такого круглого стола будет создан объемный рабочий документ. Эти рабочие документы содержат краткое описание проблемы, а затем рассматривают конкретные теоретические и практические вопросы, касающиеся прозрачности, контроля и надзора, ответственности и демократического управлением в целом. Разумеется, эти документы не предполагают решения вопросов, которые в них рассматриваются, а лишь обеспечивают фундамент, на котором будет строиться дальнейшая работа и научные исследования. Таким образом, они поднимают гораздо больше вопросов, чем предлагают ответов. Помимо этих рабочих документов, в рамках проекта подготовлен еще один доклад, не вошедший в серию «Горизонт 2015». Он называется «Тенденции и вызовы международной безопасности – Общий обзор» и описывает нынешний ландшафт безопасности и, таким образом, определяет общую основу для работы всего проекта в целом.

Бенджамин С. Бакленд, Фред Шрайер, Теодор Х. Винклер, *Демократическое управление и вызовы кибербезопасности* (Женева: Женевский центр демократического контроля над вооруженными силами, 2013).

DCAF HORIZON 2015 WORKING PAPER NO. 1.RU

Язык оригинальной версии: английский, Женева, 2009

Русская версия, 2013

Женевский центр демократического контроля

над вооруженными силами

<www.dcaf.ch>

P.O.Box 1360, CH-1211 Geneva 1, Switzerland

Дизайн обложки: Ангел Недельчев

ISBN 978-92-9222-223-9

Женевский центр демократического контроля над вооруженными силами (ДКВС)

ДКВС был основан в 2000 году швейцарским правительством. ДКВС – международная организация, в которую входят 58 государства и швейцарский кантон Женева. Главными подразделениями ДКВС являются отделы исследовательских, оперативных и специальных программ. Штат Центра составляют около 90 человек из более чем 32 стран. Штаб-квартира ДКВС находится в Женеве, Швейцария. Центр имеет постоянные представительства в Брюсселе, Любляне, Рамалле и Бейруте.

Женевский центр демократического контроля над вооруженными силами является одной из ведущих организаций в мире в сфере реформирования сектора безопасности (SSR) и управления сектором безопасности (SSG). ДКВС предоставляет странам консультативную поддержку, проводит программы практической помощи, разрабатывает и продвигает соответствующие демократические нормы на международном и национальном уровнях, пропагандирует передовой опыт и вырабатывает рекомендации для обеспечения эффективного демократического управления сектором безопасности.

Партнерами ДКВС являются правительства, парламенты, институты гражданского общества, международные организации и ряд ведомств сектора безопасности – полиция, суды, спецслужбы, пограничные и военные службы.

www.dcaf.ch

Публикация этой книги была осуществлена с содействием Управления по вопросам политики безопасности (SIPOL), Федеральный департамент обороны, гражданской защиты и спорта Швейцарии.

ISBN 978-92-9222-223-9