ЖЕНЕВСКИЙ ЦЕНТР ДЕМОКРАТИЧЕСКОГО
КОНТРОЛЯ НАД ВООРУЖЕННЫМИ СИЛАМИ (DCAF)

КИБЕРБЕЗОПАСНОСТЬ: ДОРОГА, КОТОРУЮ ПРЕДСТОИТ ПРОЙТИ

Фред Шрайер, Барбара Викс,
Теодор Х. Винклер

Женевский центр демократического контроля над вооруженными силами (DCAF)

DCAF HORIZON 2015 WORKING PAPER No. 4.RU

КИБЕРБЕЗОПАСНОСТЬ:

ДОРОГА, КОТОРУЮ ПРЕДСТОИТ ПРОЙТИ

Фред Шрайер, Барбара Викс, Теодор Х. Винклер

ЖЕНЕВА – 2013

Фред Шрайер, Барбара Викс, Теодор Х. Винклер, *Кибербезопасность: дорога, которую предстоит пройти* (Женева: Женевский центр демократического контроля над вооруженными силами, 2013).

DCAF Horizon 2015 Working Paper No. 4.RU

Оригинальное издание на английском языке, 2011
Русская версия, 2013
Исполнительный издатель: ООО Прокон, http://procon.bg
Дизайн обложки: Ангел Недельчев
ISBN 978-92-9222-235-2

КИБЕРБЕЗОПАСНОСТЬ:

ДОРОГА, КОТОРУЮ ПРЕДСТОИТ ПРОЙТИ

Фред Шрайер, Барбара Викс, 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.

СОДЕРЖАНИЕ

Предисловие

Открытый Интернет – дар человечеству. Он не только предоставил возможность ученым, компаниям и различным организациям стать более эффективными, но и обусловил беспрецедентный обмен идеями, информацией и культурами среди ранее разъединенных людей и групп. Интернет произвел глобальную революцию в ведении бизнеса, взаимодействии и общении.

Киберпространство определяется многообразием соединений, что одновременно переводит его в категорию зоны риска. Все возрастающие размеры, охват и функции увеличивают возможности как законопослушных граждан, так и враждебных игроков. Сопернику необходимо лишь атаковать слабейшее звено сети, чтобы завоевать новый плацдарм и получить преимущества. Кажущиеся локальными проблемы могут нарастать и быстро распространяться, создавая угрозы и системные риски.

Уязвимость в киберпространстве является реальной, серьезной и быстро разрастающейся. Объекты инфраструктуры особой важности, разведка, коммуникации, командование и контроль, торговля и финансовые операции, логистика, ликвидация последствий и готовность к чрезвычайным ситуациям полностью зависят от ИТ-систем, объединенных в сети. Нарушения кибербезопасности, кража данных и интеллектуальной собственности не знают границ. Они оказывают влияние на все – от личной информации до государственных тайн.

В данной работе рассмотрены пути вероятного развития этих проблем, а также предлагаются некоторые способы их решения на государственном и международном уровнях.

1. О предмете исследования

1.1. Киберпространство

Киберпространство, пятое поле битвы (после земли, моря, воздуха и космоса), состоит из всех компьютерных сетей мира и всего, что они соединяют и контролируют при помощи кабельных, оптоволоконных и беспроводных соединений.[1] Это не просто Интернет – открытая сеть сетей. В киберпространство входят кроме Интернета многие другие компьютерные сети, включая и те, к которым, по идее, нельзя подключиться через Интернет. Некоторые из этих частных сетей выглядят как Интернет, но они, по крайней мере теоретически, изолированы. К другим компонентам киберпространства относятся транснациональные сети, которые занимаются передачей данных о денежных потоках, торгах на фондовых биржах и операциях по кредитным картам. Кроме того, существуют системы контроля и получения данных, которые позволяют машинам «общаться» с другими машинами, например, панели управления, «разговаривают» с помпами, лифтами и генераторами. Это явление известно как «Интернет вещей», в котором неодушевленные объекты могут общаться друг с другом, часто при помощи технологии РЧИ (радиочастотной идентификации).

Киберпреступники могут взломать такие сети и уничтожить их, либо взять под свой контроль. В случае завладения сетью возникает угроза кражи всей информации либо внедрения инструкций, согласно которым будут переводиться деньги, выливаться нефть, выпускаться газ, взрываться нефтеперерабатывающие заводы, трубопроводы и генераторы, сходить с рельс грузовые поезда и вагоны метро, либо произойдет досрочный взрыв ракеты (или ее направят не в то место). Если сети будут уничтожены, данные стерты, а компьютеры превращены в пассивных воинов (бот-сеть), тогда могут обрушиться финансовые системы, нарушиться системы поставок, энергоснабжение будет отключено, спутники сойдут со своих орбит в космосе, прервется авиасообщение. Утрата доверия к финансовой информации и электронным переводам может привести к проблемам в экономике. Утрата контроля всего на несколько дней может привести к серии экономических проблем в условиях нехватки денег и пищи.

Такое уже случалось, иногда в результате эксперимента, иногда в результате ошибки, а иногда и в результате кибервойны или киберпреступлений. Информация, которая находится в компьютерных сетях, управляющих энергоснабжением, транспортом, банками и финансами, коммуникациями, охраной здоровья, личными либо корпоративными данными и государственными секретами, может быть использована и подвергнуться атаке, ведущейся из отдаленных мест. Многие аспекты киберпространства делают такой вариант возможным, включая промахи в самой системе Интернета, ошибки аппаратного оборудования и программного обеспечения, желание использовать в режиме он-лайн еще более важные системы, нехватка эффективных средств сдержи-

[1] Все концепции, использованные в данной работе находятся в свободном доступе по условиям лицензии Creative Commons (Поль Гарленд, Деа Пиджей, Миксан, Нико Кайзер и Анаксила).

вания и отсутствие соответствующих механизмов защиты. Угрозы в киберпространстве многочисленны и разнообразны, как и само киберпространство. Они заложены в самой природе сети: их взаимосвязанность, масштаб, скорость и сложность понимания происходящего – все это характеризует случаи киберугроз. Не существует безусловной защиты от кибератак, которые совершаются не только из-за границы, но и за пределами физического пространства, в цифровом эфире киберпространства. Широкополосный Интернет сделал возможным увеличение скорости атак, и организации даже не успевают начать исправлять свои системы, чтобы защититься. В результате, анонимно провести разрушительную кибератаку все легче, а защититься от таких атак – все сложнее и дороже. Эта все возрастающая асимметрия серьезно меняет условия игры. Современный вор с помощью компьютера может украсть больше денег, чем с помощью оружия. Завтрашний террорист сможет причинить больше ущерба с помощью клавиатуры, чем применив бомбу. Эти проблемы уже сложились и вряд ли изменятся в ближайшее время.

1.2. Киберпреступление

Киберпреступления – угроза сегодняшнего дня, превратившаяся в тихую всемирную цифровую эпидемию. Понятие *киберпреступление* включает в себя целый ряд правонарушений, в том числе взлом компьютеров, данных и систем (хакерство); совершаемые при помощи компьютера фальсификации и мошенничества, такие как фишинг и фарминг;[2] правонарушения в области контента, такие как детская порнография и нарушение авторских прав путем распространения пиратского контента. Киберпреступления возникли как результат желания кибервандалов продемонстрировать свое преимущество и быстро стали высоко прибыльным преступным бизнесом. Существует все более очевидная связь между киберпреступностью и другими угрозами, такими как промышленный шпионаж, деятельность иностранных разведывательных служб и терроризм.

Как и в других аспектах глобализации, быстрое развитие Интернета опередило развитие регуляторных механизмов, что привело к дальнейшим нарушениям. Атаки киберпреступников становятся все более регулярными, сложными и изощренными; все чаще они выявляются уже после совершения, если вообще выявляются. Киберпреступники атакуют организации и частных лиц при помощи вредоносного программного обеспечения и анонимизации, что позволяет обойти существующие меры безопасности. Нынешние системы наблюдения за проникновением, базы данных вирусов и антивирусные программы не обеспечивают необходимый уровень защиты и слишком быстро устаревают. Таким образом, с выгодой для себя киберпреступники применяют инновации так быстро, что многие правительства, организации и разработчики систем информационной безопасности не успевают за ними.

Более того, киберпреступники в настоящее время могут атаковать самое слабое звено большинства моделей безопасности (конечного пользователя) через Интернет при помощи социальной инженерии. Используя мошенничество и различ-

[2] Фишинг и фарминг – две популярные формы мошенничества, цель которых – заставить жертву поверить, что она находится на безопасном сайте, например, банка, тогда как, в действительности, она зашла на поддельный сайт, созданный для похищения личных данных и денег пользователя.

ные уловки, они заставляют жертву поверить в то, что она коммуницирует с коллегой, клиентом либо другим легитимным участником. Постоянно совершенствующиеся методы достижения «невидимости» позволяют киберпреступникам действовать, не опасаясь своевременного обнаружения, не говоря о задержании и судебном преследовании.

За последние три года резко возросло количество кибератак, совершаемых при помощи вредоносного программного обеспечения. Большая часть этих атак проводилась в отношении финансового сектора, их целью были компьютеры финансовых учреждений.[3] Другие виды киберпреступлений, в особенности нарушение закона об интеллектуальной собственности, привлекательны для других криминальных групп, к которым относятся давно существующие организованные группы киберпреступников, действующие в таких сферах, как пиратство в области программного обеспечения, всевозможные нарушения авторских прав.

Все большее число создателей вредоносного программного обеспечения и киберпреступников, которых можно нанять, предлагает другим киберпреступникам свои умения, способности, продукты и услуги: получение и хранение данных, незаметный доступ к системам, кража личности; неправильные переадресация, идентификация пользователя при работе на клавиатуре, подтверждение личности и бот-сети. Среди преимуществ, предлагаемых преступникам киберпространством, – анонимность и возможность создавать транснациональные объединения, связь между участниками которых доказать крайне сложно. Таким образом, вокруг похищения, хранения и перепродажи информации возникла подпольная экономика.

Существуют, по крайней мере, три причины, по которым киберпреступность в целом и организованная киберпреступность в частности будут и дальше развиваться в ближайшее время. Во-первых, технологии для совершения киберпреступлений стали более доступными. Программные инструменты можно приобрести он-лайн, что дает возможность пользователю идентифицировать открытые порты или обойти пароли и другие меры безопасности. Такие инструменты делают правонарушителями большое число людей, не имеющих особых компьютерных способностей. Например, у авторов недавно обнаруженной бот-сети «Марипоза», возможно, крупнейшей на данный момент, не было особых хакерских навыков.[4] Во-вторых, изменяется посетитель Сети. В 2005 году количество пользователей Интернета в развивающихся странах было значительно выше, чем в развитых странах. Даже если эти новые пользователи и не склонны становиться преступниками, число правонарушителей будет расти, тогда как число богатых жертв из более благополучных регионов будет оставаться примерно тем же. В результате, интенсивность атак на эти субъекты, скорее всего, возрастет, так как Интернет и широкополосные коммуникации сделали их такими же доступными для преступников, как и местных состоятельных субъектов.

В-третьих, благодаря применению автоматических систем и расширению диапазона частот, количество атак может расти в геометрической прогрессии. За короткий промежуток времени при помощи автоматического управления могут быть разосланы миллионы единиц спама. Хакерские атаки в настоящее время

---

[3] Economic and Social Council, ECOSOC/6444, 37th & 38th Meetings, Council briefed on Cybersecurity, 16 July 2010, p. 1.

[4] Charles Arthur, “Alleged controllers of ‘Mariposa’ botnet arrested in Spain,” *Guardian*, 3 March 2010.

также автоматизированы; ежедневно происходит до 80 миллионов попыток атаковать компьютеры с применением программных инструментов, позволяющих совершить тысячи атак за короткий промежуток времени. Недавно была обнаружена бот-сеть, которая проводила миллионы автоматизированных атак и контролировала 12,7 миллионов компьютеров, многие из которых принадлежали крупнейшим мировым корпорациям.[5] Кроме всего прочего, схемы, подобные этой, позволяют киберворам совершать кражи незаметно, снимая незначительное количество средств со счетов многочисленных жертв, что снижает вероятность обнаружения преступников.

Доход от киберпреступлений значительно превысил доход от других преступлений, включая торговлю наркотиками. По некоторым оценкам, потери общества составляют ежегодно около 750 миллиардов Евро[6] в Европе и 1 триллион долларов в США[7] – цифры, возможно, преуменьшеные из-за недостатка точной информации о реальных вмешательствах и связанных с ними финансовых потерях.[8] И все же, есть сомнения в точности этих оценок.

1.3. Национальная кибербезопасность: основные проблемы и стратегические вызовы

Открытый Интернет – дар для человечества. Он не только предоставил возможность ученым, компаниям и различным организациям стать более эффективными, но и обусловил беспрецедентный обмен идеями, информацией и культурами среди ранее разъединенных людей и групп. Интернет произвел глобальную революцию в ведении бизнеса, взаимодействии и общении.

Киберпространство определяется многообразием соединений, что одновременно переводит его в категорию зоны риска. Все возрастающие размеры, охват и функции увеличивают возможности как законопослушных граждан, так и враждебных игроков. Сопернику необходимо лишь атаковать слабейшее звено сети, чтобы завоевать новый плацдарм и получить преимущества. Кажущиеся локальными проблемы могут нарастать и быстро распространяться, создавая угрозы и системные риски.

---

5 United Nations Office on Drugs and Crime (UNODC), *The Globalisation of Crime. A Transnational Organised Crime Threat Assessment* (Vienna: UNODC, 2010), p. 204.

6 Еврокомиссия считает, что правительства и общество теряют около 750 миллиардов Евро ежегодно, и эта сумма растет. Европол и Европейское агентство по сети и информационной безопасности, «Enisa», не называют цифры из-за отсутствия единого Европейского определения киберпреступления, а также из-за постоянного увеличения суммы ущерба.

7 UNODC, *The Globalisation of Crime,* op. cit., p. 204. В эту цифру входят потери от кражи интеллектуальной собственности и потери компаний, а не прибыли преступников.

8 При совершении киберпреступления, менее половины от общего числа жертв обращается в свои финансовые учреждения или полицию, и только треть обращается к владельцу веб-сайта или поставщику услуг. *Norton Cybercrime Report: The Human Impact* (Mountain View, CA: Symantec Corporation, 2010).

Растущая угроза

Несмотря на постоянные напоминания об уязвимости ИТ-оборудования и Интернета и многомиллионные суммы, которые идут на защиту электронных сетей, риск атак со стороны киберпреступников продолжает неуклонно возрастать. Растущая угроза и увеличение числа сообщений о проникновениях в компьютерные системы правительственных учреждений и коммерческих компаний подчеркивают уязвимость взаимосвязанных сетей, а также необходимость развития глобальной системы безопасности и управления киберпространством. Глобальные аспекты киберпространства являются основной проблемой обеспечения безопасности всех стран. Пока эти проблемы не решены должным образом, государства будут по-прежнему не в состоянии обеспечить свою национальную и экономическую безопасность, безопасность своего народа в киберпространстве. Тренды киберпреступности требуют более серьезного реагирования:

- ✓ Атаки киберпреступников и нарушения систем безопасности будут происходить чаще, станут сложнее и изощреннее; все чаще они будут выявляться постфактум, если вообще будут;
- ✓ Многое указывает на то, что будущие атаки киберпреступников станут более серьезными и комплексными, их будет сложнее предотвратить, отследить и изучить;
- ✓ Сейчас не существует эффективных механизмов сдерживания киберпреступности, они недоступны для большинства пользователей, многие из которых все еще недооценивают масштаб и серьезность проблемы;
- ✓ Недостаток обращений к регулирующим и правоохранительным органам по поводу проникновения в систему является первопричиной того, что вопросы кибербезопасности и киберпреступности не признаются первоочередными и приоритетными.

Уязвимость в киберпространстве является реальной, серьезной и быстро разрастающейся. Объекты инфраструктуры особой важности, разведка, коммуникации, командование и контроль, торговля и финансовые операции, логистика, ликвидация последствий и готовность к чрезвычайным ситуациям полностью зависят от ИТ-систем, объединенных в сети. Нарушения кибербезопасности, кража данных и интеллектуальной собственности не знают границ. Они оказывают влияние на все – от личной информации до государственных тайн.

Враждебные игроки различны по своему потенциалу, масштабности, намерениям, источнику и ресурсам. Это могут быть и иностранные правительства, разведывательные службы и военные; хорошо организованные и финансируемые негосударственные игроки, такие как организованная преступность и террористические группы; отдельные хакеры и преступники, а также недовольные сотрудники и другие инсайдеры. Все они могут использовать Интернет, чтобы причинить физический вред и нарушить основные элементы цифровой инфраструктуры.

Стратегические вызовы

- ✓ Угрозы в киберпространстве являются наиболее серьезными для национальной и экономической безопасности, с которыми сталкиваются государства. Кибербезопасность станет ключевой проблемой в экономическом, политическом, социальном и военном аспектах. Тем не менее, она остается наименее понятной и наиболее недооцененной угрозой.
- ✓ Сама сложность угрозы мешает пониманию ее последствий и проведению конструктивного обсуждения необходимых стратегий реагирования.
- ✓ Кибербезопасность – многосторонняя проблема, которая затрагивает все аспекты жизни современного общества и экономики. В связи с этим сложно определить конкретные угрозы и необходимые меры противодействия.
- ✓ Организованную преступность все больше будут привлекать возможности злоупотреблений, манипуляций и даже доминирования в киберпространстве.
- ✓ Необходимо большее понимание того, что киберпространство в настоящее время является самым важным театром военных действий. Борьба за кибердоминирование – и соответственно способность противостоять кибератакам – означает новую эру военных взаимоотношений, которая существенно изменит природу и структуру вооруженных сил. В обозримом будущем на смену кинетической энергии как ключевому компоненту военной мощи придет киберэнергия.
- ✓ Всеобъемлющий характер киберпроблем в современной жизни потребует не только военного ответа на возникшую угрозу, но и всеобъемлющей стратегии, разработанной всем сектором безопасности. Растущая значимость киберкомпонента будет, среди прочих, одной из основных движущих сил реформы сектора безопасности – и одной из наиболее сложных проблем управления сектором безопасности.
- ✓ Кибербезопасности нельзя достичь на уровне государства. Она требует интеграции усилий и частного сектора, и предприятий, международной координации и сотрудничества в беспрецедентных масштабах.
- ✓ Если не решить проблему обеспечения кибербезопасности, последствия могут быть очень серьезными. Существует реальная угроза того, что Интернет, суть глобализирующегося мира, станет либо дисфункциональным, либо распадется на несколько отдельных внутренних сетей. В любом случае, экономические, финансовые, социальные, политические последствия и последствия в сфере безопасности будут масштабными.

Более того, киберпространство является идеальным полем для асимметричной войны. Отдельных людей либо группы привлекают очень низкая стоимость и относительно низкий уровень технической подготовки, необходимый для проведения атак на важные правительственные, экономические, финансовые и военные объекты. В 2008 году, накануне нападения России на Грузию с применением обычного оружия, серия кибератак вывела из строя грузинские правительственные, медийные и военные объекты, показав «лицо будущих войн».

2. Реагирование

2.1. Обзор

Политики, руководители предприятий и эксперты признают и понимают растущую уязвимость сетей. Мы зависим от них практически во всем: трансакции, обмены, защита важнейших объектов инфраструктуры, безопасность, мобильность, банковские операции и ведение бизнеса. И программное обеспечение, и оборудование, и все риски, возникающие по вине пользователей – все это было предметом обсуждения долгие годы. К сожалению, на данный момент, после многочисленных инициатив и консультаций, все еще не наблюдается заметного прогресса в создании эффективной и действенной глобальной системы реагирования на киберпреступления и киберугрозы. Причинами этого, в основном, являются следующие:

- ✓ Отсутствие соответствующих стимулов (или ответственности) создателей технологий и программного обеспечения за интегрирование элементов безопасности, необходимых для защиты потребителя.
- ✓ Нереалистичные ожидания, что конечный пользователь может, хочет или обладает достаточными знаниями, чтобы нести ответственность за безопасность своего компьютера или мобильного устройства, а также, следовательно, и сети.
- ✓ Различные правовые системы и законы, относящиеся к киберпреступлениям и кибербезопасности; у некоторых стран нет законов, которые относятся к законодательству в области киберпреступлений и кибербезопасности, тогда как законы других держав в этой сфере относительно современны. Всегда будет существовать проблема определения такого преступления в различных правовых системах. Но без, как минимум, единой международной стратегии «отслеживания и контроля прохождения», возможности поймать преступников весьма незначительны.
- ✓ Отсутствие последствий/санкций для киберпреступников, что связано с проблемой применения закона и назначения наказания на территории одной страны за преступление, совершенное в мире без границ (в Интернете). Это особенно сложно сделать тогда, когда у многих стран нет даже законодательства, определяющего сущность киберпреступления.
- ✓ Неспособность некоторых правительств к сотрудничеству в связи с приоритетами их национальной безопасности.
- ✓ Недостаточное количество сообщений и отсутствие мониторинга киберпреступлений, вредоносного ПО и он-лайн мошенничества.
- ✓ Развивающиеся страны не могут в достаточной степени финансировать необходимые меры по обеспечению кибербезопасности; без этого глобальная система остается крайне уязвимой.
- ✓ Нехватка подготовленного персонала.

Комплексность проблемы делает особенно сложной задачу создания системы всеобъемлющего эффективного реагирования, приемлемой для всех сторон. Некоторые субъекты, например ITU (Международный союз электросвязи), призывают к подписанию международного кибердоговора, другие предлагают национальный или пошаговый подход, определяемый сектором и направлен-

ный на создание потенциала. Оптимальным решением, без сомнения, будет, как и в других сферах, скоординированное сотрудничество международных и национальных организаций, законодателей, представителей различных секторов, государственных, частных компаний и конечных пользователей. Оптимальным решением станет Международная стратегия (подобная, в принципе, Женевской конвенции по традиционной войне), которой должны придерживаться все страны, создавая национальные регуляторные органы, общественно-государственные объединения (в особенности по защите исключительно важных объектов инфраструктуры), инициативы частного сектора и конечных пользователей. Достижимо ли это? А развивающиеся, слаборазвитые и недееспособные государства? Кто является ключевыми игроками, с какого рода проблемами они сталкиваются? Кто должен сделать все необходимое для достижения кибербезопасности?

2.2. Ключевые игроки

2.2.1. Правительства

Государства несут юридическую, организационную и политическую ответственность за обеспечение кибербезопасности. Так как кибербезопасность и защита важной информации и инфраструктуры лежат в основе безопасности и процветания государств, руководство обеспечением безопасности должно инициироваться наивысшими уровнями государственной власти. Правительству следует определить сферы ответственности и подотчетности, обеспечить контроль и непрерывность всех необходимых действий. Оно должно быть во главе системы всеобъемлющего реагирования, чтобы обеспечить превосходство страны в киберпространстве, уменьшать риски, используя для этого все возможности при помощи усовершенствования знаний и процесса принятия решений. На уровне страны этот подход предполагает совместную ответственность, требующую скоординированных действий, связанных с предупреждением, подготовкой, реагированием и ликвидацией последствий со стороны всех министерств и правительственных учреждений, а также частного сектора и граждан. На региональном и международном уровне этот подход означает координацию и сотрудничество со всеми основными партнерами. И именно правительство должно отобрать самых высококвалифицированных и подготовленных сотрудников, способных возглавить и направить эту работу.

К основным элементам политической ответственности государства относятся следующие: создание стратегии кибербезопасности, которая соответствовала бы основным принципам стратегии национальной безопасности; создание соответствующей правительственной программы по разработке стандартов, политики и руководства в сфере обеспечения доступности и безопасности информации, а также быстрого восстановления систем; предоставление соответствующего финансирования; накопление опыта и знаний, необходимых правительству, промышленности и обществу для обеспечения безопасности страны; проведение соответствующих исследований, направляемых, координируемых и используемых наилучшим образом. Кроме того, политическая ответственность государства предполагает обеспечение международного сотрудничества, координации и гармонизации усилий в сфере безопасности киберпространства.

К организационной функции государства относится принятие всех мер по обеспечению безопасности важнейшей инфраструктуры и создание соответствующих возможностей реагирования. Так как компьютерные сети в настоящее время используются на всех правительственных уровнях для обеспечения национальной и общественной безопасности, экономического процветания, деятельность правительства зависит от информационно-технологических систем, которые должны быть хорошо защищены от незаконного проникновения и нападений. Растущая частота и сложность атак на важнейшие объекты инфраструктуры и ключевые ресурсы обусловливают не только необходимость тщательного планирования на национальном, региональном и местных уровнях, но также предполагают создание новых структур, организаций и инструментов, обеспечивающих подготовку к событиям, способных подорвать действия правительства по предоставлению населению основных услуг, реагированию на эти события, а также возможности ликвидации последствий деятельности террористов или природных катастроф.

Вызовы правительствам

Достижения стран в защите своих киберпространств и ключевой информационной инфраструктуры несопоставимы. Тогда как такие страны, как Великобритания, Австралия, Канада, Финляндия, Франция, Бельгия, Израиль и США разработали Стратегию кибербезопасности и создали национальные системы защиты киберпространств и ключевой информационной инфраструктуры, другие страны все еще пытаются выработать единый подход.

Особую обеспокоенность вызывает недостаток ресурсов для разработки и создания эффективных систем обеспечения кибербезопасности у развивающихся, слаборазвитых и недееспособных стран. Если все страны не примут участия в этом процессе, единая система останется уязвимой для атак. Различия национальных «киберпотенциалов» серьезно мешают международному сотрудничеству. На данный момент существует «киберпропасть» между странами ОЭСР (Организации экономического сотрудничества и развития) и большей частью Африки. Из этих различий можно извлечь пользу – и, следовательно, усугубить проблемы стран ОЭСР, что, в конечном счете, поставит под угрозу перспективы экономического развития Африки. Ведь в целом, с точки зрения кибербезопасности, мы сильны настолько, насколько сильно наше слабейшее звено.

С некоторыми исключениями, правительства, реагируя на угрозы и риски киберпространства, избирали два подхода – правовой и организационный. Ни один не был последовательным и согласованным; более того, эти подходы менее взаимосвязаны, чем того хотелось бы. Отсутствие руководящего центра, организационной стабильности и опыта – основные факторы, ограничивающие способность к реагированию. Самые серьезные препятствия в работе правительств лежат в правовой сфере, где сама природа киберпространства противоречит основным принципам юриспруденции, гражданской и военной, внутренней и международной.

Улучшению ситуации не способствует случайный интерес к вопросам кибербезопасности со стороны законодательных органов всех стран. Законодательные органы не обращаются к вопросам кибербезопасности систематически, а лишь от случая к случаю.

Исследование McAfee, 2010 г. [9]

McAfee, самая крупная в мире компания-разработчик антивирусного программного обеспечения, провела опрос 600 руководителей отделов информационных технологий и безопасности предприятий важнейшей инфраструктуры отраслей энергетики, транспорта, водоснабжения и водоотвода, телекоммуникаций, а также финансового сектора и правительственных учреждений в 14 странах. Все они давали детальные ответы на вопросы о более чем 24-х мерах безопасности – технологиях, политике, процедурах и их использовании. В докладе подробно описано как субъекты, ответственные за защиту объектов важнейшей инфраструктуры, реагируют на кибератаки, пытаясь обеспечить безопасность и работая совместно с правительствами.

Обобщение этих данных показывает, какие страны и секторы в наибольшей и наименьшей мере применяют меры безопасности. Эти данные не обязательно являются показателем качества безопасности в секторе или стране, но позволяют объективно судить о применяемости практик и мер обеспечения безопасности. Проведенное исследование позволило сделать вывод о том, что наилучший показатель – 62% присущ Китаю, что намного превышает показатели США, Великобритании и Австралии (которые стоят следующими в рейтинге с результатами 50-53%). Италия, Испания и Индия имеют наихудшие показатели (менее 40%), тогда как Япония, Россия, Франция, Саудовская Аравия, Мексика, Бразилия и Германия набрали по 40-49%. Меры обеспечения безопасности чаще применяются в банковском и энергетическом секторах, тогда как самый низкий показатель у сектора водоснабжения и водоотвода.

Владельцы и операторы объектов важнейшей инфраструктуры всего мира сообщают, что их сети и системы контроля являются объектами постоянных атак. В докладе указано, что 54% объектов стали жертвами крупномасштабных воздействий – от массированных DDos-атак (отказ в обслуживании), целью которых является отказ систем, до попыток незаметного проникновения в систему. 60% опрошенных считают, что иностранные правительства принимают участие в атаках на объекты важнейшей инфраструктуры их стран. Наибольшую угрозу представляют, по их мнению, США (36%) и Китай (33%). Кроме того, к числу киберпреступников относят и индивидуалов-хакеров, и е-вандалов (электронных вандалов), и организованные преступные группы. Широко распространены атаки с целью получения финансовой выгоды, такие как вымогательство и хищение услуг. Последствия кибератак различны, но в некоторых случаях они были достаточно значимыми, включая серьезные эксплуатационные отказы.

В докладе также указывается, что риск кибератак возрастает. Более трети руководителей отделов информационных технологий (37%) отметили, что уязвимость их сектора возросла за последние 12 месяцев, а две пятых ожидают серьезных атак на свой сектор в течение следующего года. Только 20% опрошенных считают, что их сектор защищен от серьезных кибератак на ближайшие пять лет.

---

[9] Stewart Baker, Shaun Waterman и George Ivanov, “In the Crossfire: Critical Infrastructure in the Age of Cyber War,” Доклад по заказу McAfee подготовлен Центром стратегических и международных исследований (CSIS), Santa Clara, CA, McAfee, Inc., 2010.

По оценкам, стоимость простоя в результате серьезных атак превышает 6 миллионов долларов США в день, а в таких секторах как нефтегазовый, – 8 миллионов долларов в день. Кроме финансовых потерь, серьезный ущерб от атак – испорченная репутация, что обусловлено утратой персональной информации. Только по этой причине о большинстве случаев кибератак не сообщают. Кроме этого, в докладе опубликованы следующие выводы:

- ✓ Безопасность – основной фактор принятия решений относительно политики в сфере информационных технологий и инвестиций в эту отрасль: 92% опрошенных заявили, что безопасность либо «жизненно необходима», либо «очень важна». Как «жизненно необходимую» безопасность чаще всего оценивали руководители Китая и США.
- ✓ Существует низкая степень уверенности в готовности отражать кибератаки: более трети респондентов считает, что их сектор не готов справиться с масштабными атаками или тайным проникновением со стороны серьезных соперников. Наименьшую уверенность в степени готовности высказали Саудовская Аравия (90%), Мексика (75%) и Индия (68%), тогда как Германия (78%) и Великобритания (64%) проявили наибольшую уверенность. Есть сомнения в способности правительств предотвратить и сдержать атаки: 45% респондентов считают, что их правительства не способны полностью предотвратить и сдержать кибератаки. Две трети опрошенных из Бразилии и Италии считают свои правительства не способными противодействовать кибератакам. Только китайские и американские респонденты уверены в возможности своих правительств.
- ✓ Существуют также сомнения в способности самих провайдеров важнейшей инфраструктуры предоставлять бесперебойные услуги в случае серьезной кибератаки: 30% респондентов не уверены в том, что их банк или другой поставщик финансовых услуг сможет обеспечить надежность услуг. 30% высказывают подобные сомнения в отношении своих телекоммуникационных провайдеров. Уверенность в противодействии атакам самая низкая в Италии, Франции и Испании.
- ✓ Связанные с рецессией сокращения увеличивают риск: две трети руководителей отделов информационных технологий говорят, что экономический климат в настоящее время привел к сокращению выделяемых на безопасность ресурсов. Особенно заметны сокращения в нефтегазовом секторе в таких странах, как Индия, Испания, Франция и Мексико, в наименьшей степени – в Австралии.
- ✓ Законы неэффективны в защите от потенциальных атак: 55% опрошенных считают, что законы их стран неадекватны при сдерживании потенциальных кибератак; наиболее скептичны представители России, Мексики и Бразилии; наибольше доверие к законам выражают представители Германии, затем – Франции и США. 45% респондентов не верят, что власти способны предотвратить и сдержать атаки.
- ✓ Основная доля расходов, связанных с последствиями кибератак, приходится на страховые компании: более половины опрошенных ожидают, что страховые компании покроют потери от кибератак. В данном случае следует заметить, что практически не существует страхования от кибератак.

В правовой сфере ответственность государства состоит в том, чтобы создать систему защиты важнейшей инфраструктуры и разработать законы о преступлениях в киберпространстве. Главная обязанность государства в области

права происходит от давно признанного принципа международного права – «государство обязано усердно предотвращать совершение уголовных преступлений в отношении других стран и их народов». Этот принцип нашел свое отражение во многих государственных декларациях, судебной практике и работах виднейших ученых. Из государственной и международной практики, которые лежат в основе международного обычного права, вытекает обязанность государств предотвращать атаки в отношении других государств негосударственных структур. Терпимость к таким атакам, с точки зрения международного права, является преступлением. Кроме того, правительства должны защищать частную жизнь и гражданские свободы, а также соответствующим образом обеспечить защиту информации.

2.2.2. Законодательные органы

Необходимость законодательного контроля над всеми действиями, предпринимаемыми правительством и финансируемыми налогоплательщиками, обусловила создание в большинстве стран парламентских комитетов, в задачи которых входит обеспечение контроля над действиями по обеспечению безопасности киберпространства и защиты объектов важнейшей инфраструктуры страны. В некоторых странах эти комитеты осуществляют контроль над сектором «национальной безопасности», тогда как в других – отвечают за контроль над всеми правительственными структурами, которые используют электронные сети и информационные технологии для обеспечения национальной безопасности, а также экономического благосостояния. На практике задачи и обязанности таких комитетов не являются ни очевидными, ни четко определенными. Над чем же конкретно должны осуществлять надзор эти комитеты? Есть ли у членов этих комитетов необходимые знания, понимание, компетентность и подготовка для осуществления законодательного контроля над столь сложной сферой? Комитеты часто не в состоянии выполнить свою основную миссию – обеспечить принятие законов, которые соответствуют современным вызовам со стороны киберпреступников. Так как технологии развиваются и возникают новые угрозы, законодатели должны хотя бы обеспечить модернизацию законов о киберпреступлениях, их соответствие новым угрозам.

Могут понадобиться более профессиональные и эффективные способы и средства помощи парламенту, позволяющие справиться с этой достаточно трудной задачей контроля над всеми мерами по предотвращению, подготовке, реагированию и восстановлению после кибератак. Содействие в этом вопросе должно исходить от всех министерств, правительственных агентств и частного сектора. Более всего необходимо улучшить взаимопомощь и международное сотрудничество в области киберпреступлений между правительствами, промышленностью и НПО. Существует также необходимость проведения консультаций по вопросам технологий, бизнес-процедур и политической поддержки лидеров как в институтах исполнительной, так и законодательной власти, а также для решения проблем обеспечения безопасности киберпространства и защиты объектов важнейшей инфраструктуры. Необходимо тесное сотрудничество с отраслями важнейшей инфраструктуры, цель которого – помочь правительству и промышленности понять ценность общественно-государственных объединений, обозначить необходимые шаги в сфере безопас-

Вызовы законодательным органам

- ✓ Техническая сложность вопроса обнаруживает недостаточность знаний большинства членов парламента, что предполагает привлечение высококлассных специалистов. Эти действия могут себе позволить немногие парламенты.
- ✓ Отнесенность кибербезопасности к многосторонней проблеме мешает поместить ее в рамки существующей структуры комитетов. Возникает вопрос: кто ответственен за решение этой проблемы – комитет по вооруженным силам или комитет по безопасности? Юстиция, полиция или комитет по национальной безопасности? Комитет по телекоммуникациям? Или они все? И какова роль комитета по иностранным делам?
- ✓ Некоторые страны приняли «киберстратегию». Что должно быть мерилом эффективности действий в этой сфере?
- ✓ Кибербезопасностью, в полной мере или частично, занимаются государства при помощи военных и/или разведывательных служб – т.е. при помощи агентств, которые по своей природе непрозрачны и закрыты.
- ✓ Даже самая основная задача парламента, а именно однозначно определить – подверглась ли страна иностранному военному нападению и, следовательно, находится ли в состоянии войны, – в большей или меньшей мере невыполнима для большинства современных парламентов. Не существует четкого определения кибератаки. Кроме того, нападающие скрываются – в мире, где страна не несет ответственности за кибердеятельность своих граждан, – за анонимностью предположительно независимых «хакеров» и «хактивистов». Этот процесс делает страны, особенно развивающиеся, уязвимыми и представляет собой вызов для основ международного мира и порядка.

ности инфраструктуры. Правительствам нужна помощь во всех аспектах обеспечения безопасности киберпространства. Необходимо поощрять сотрудничество правительств и агентств.

2.2.3. Вооруженные силы

Вооруженные силы должны постоянно учитывать тот факт, что безопасность их сетей, систем и коммуникаций может быть нарушена, а их системы могут быть инфицированы, ими могут управлять со стороны, их функционирование может быть прервано в результате кибервойны. Вредоносный код может распространиться незаметно, создавая цифровой плацдарм, с которого данные будут переданы на серверы, находящиеся под иностранным контролем, и с которых секретная информация передается неизвестным конкурентам.

Информационные технологии и цифровая инфраструктура применяются практически во всех сферах деятельности вооруженных сил: командование и контроль над вооруженными силами, предоставление разведывательной информации, данных наружного наблюдения, радиоразведки и информации о координатах целей в режиме реального времени; системы логистики и управления. Эти технологии могут не только предоставить вооруженным силам существенное преимущество над противником, но также дать противнику информацию о намерениях и потенциале, что может помешать проведению операции или сорвать ее.

Так как кибервойна асимметрична, а средства для ее ведения дешевы, противникам не нужно создавать дорогостоящее оружие и развивать традиционные вооруженные силы, чтобы представлять собой угрозу. Небольшое число целеустремленных программистов может, если найдет уязвимое место, получить информацию о национальных вооруженных силах, украсть планы операций, заблокировать потоки разведывательной информации, нарушить системы наведения на цель или разрушить системы логистики. Поэтому многие военные разрабатывают наступательный киберпотенциал.

Тем не менее, проблема стран с развитыми вооруженными силами состоит в том, что не только у них есть наступательный киберпотенциал, но и у их противника, защиту от которого они должны обеспечить. В ядерную эру сильный наступательный потенциал должен служить оборонным целям, угрожая расплатой и, следовательно, удерживая противника от нападения. Применение этой формулы сдерживания к киберконфликтам кажется логичным, но понятие *киберсдерживание* очень несовершенно. В киберпространстве никто не может быть уверен в своей способности установить нападающих. Искушенные нападающие умеют не только скрывать свою личность, но и перекладывать ответственность на кого-то другого. Также сложно предсказать размер сопутствующего ущерба, включая и непреднамеренный ущерб субъекту и урон сетям третьих сторон, связанных с сетью пострадавшего или зависящих от нее.

Тогда как неопределенность и неуверенность всегда были частью войны, понять боевую обстановку в киберпространстве весьма сложно. И последствия неуверенности особенно важны для сдерживания киберугроз, которое предполагает ответные меры, изменяющие прибыли и стоимость атаки для противника. Сложность состоит не только в демонстрации уверенности неизвестному противнику, но и в изменившемся контексте сдерживания. Во времена Холодной войны существовала симметрия уязвимости. Этой симметрии больше нет. Развитые нации более зависимы от цифровых сетей и эта асимметричная уязвимость означает, что даже в случае «обмена» равноценными кибератаками одна из сторон потеряет больше, чем другая. Более того, анонимный противник может и не потерять ничего, так как он неизвестен, а, следовательно, и возмездие невозможно.

Угрозой возмездия гораздо труднее сдержать негосударственных оппонентов. И их готовность рискнуть будет значительно выше, чем у большинства государств, поскольку у них нет столиц, инфраструктуры либо активов, которым можно угрожать. Кроме того, на них не распространяются те политические ограничения, которые существуют для государств, действующих в киберпространстве. Некоторые акторы будут даже приветствовать месть, так как она послужит оправданием их действий и добавит им сторонников. Наилучшим доказательством слабости сдерживания в киберпространстве являются США, у которых самая лучшая наступательная киберсистема в мире, но она не дает необходимого сдерживающего эффекта.[10] Следовательно, в отличие от ядер-

[10] Среди других публикаций см. *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, TRADOC Pamphlet 525-7-8 (Department of the Army, 22 February 2010).

Вызовы вооруженным силам

- ✓ Военные стали полностью зависимы в своих действиях от киберпространства. Любая угроза из киберпространства может иметь серьезные последствия для вооруженных сил.
- ✓ Революция в военной сфере, приведшая к роботизации и точному наведению кинетической энергии, сделала армию более уязвимой перед кибератаками.
- ✓ Традиционный консерватизм военных является препятствием (в качестве исторических примеров можно привести первоначальную отрицательную оценку военными таких изобретений, как пулемет, дредноут, танк или авианосец). Есть некоторая правда в высказывании, что военные всегда готовятся к прошлой войне.
- ✓ Сила киберпространства еще не демонстрировалась в полной мере. Большинство сегодняшних угроз – продукт деятельности отдельных нарушителей и небольших организованных преступных групп. Реальный военный потенциал киберкомпонента, если он принят в качестве оружия развитой страной, был лишь слегка продемонстрирован в случаях Эстонии и Грузии и более сильно проявился в ходе недавней «Stuxnet» атаки на Иран.
- ✓ Stuxnet считается первым примером использования программного обеспечения в качестве оружия, мишенью которого становятся промышленные системы контроля. Оно должно нанести физический ущерб системам, не являющимся элементами компьютера или компьютерной сети, тем самым такие программы означают новую эру в кибервойне.
- ✓ Масштабная кибероборона требует сотрудничества частного сектора и военных.
- ✓ Если киберсоставляющая действительно заменит кинетическую энергию в качестве основного показателя военной мощи, последствия операций, их стратегия, логистика, структура, вооружение и сама природа вооруженных сил, вероятно, будут значительны.
- ✓ Прогресс в киберпространстве серьезно повлияет на относительную военную мощь стран и международный баланс сил.
- ✓ Киберпространство ставит перед военными вопросы, на которые не только нет ответов, но и сама суть которых еще не ясна.

ного оружия, сдерживающего потенциального агрессора, кибероружие не дает такого эффекта.

Для серьезного совершенствования кибербезопасности на международном уровне необходимы стратегические расчеты каждой отдельной страны по определению баланса наступательных, оборонных и многосторонних усилий, которые наилучшим образом снизят риск и увеличат стоимость кибератак. Большинство стран этого пока не сделали. Киберсдерживание привлекательно, так как оно односторонне и оправдывает создание наступательного потенциала. Но реальная безопасность может потребовать прямо противоположного подхода – многосторонних соглашений и акцента на оборону.

2.2.4. Правоохранительные органы

Международная открытость Интернета обусловливает транснациональную природу киберпреступлений. Нарушители и жертвы часто находятся в различных юрисдикциях, что представляет серьезную проблему для правоохранительных органов в расследовании и привлечении к ответственности за онлайн преступления. Несмотря на необходимость международного сотрудничества в сфере борьбы с киберпреступлениями, еще нет действительно всемирного многостороннего договора по этой проблеме. Вопросы национального суверенитета могут помешать уголовным расследованиям и сотрудничеству правоохранительных органов. Скорость, с которой киберпреступник может нанести вред и избежать обнаружения, ставит правоохранительные агентства в условия жесткого временного прессинга, обусловливая острую необходимость международного сотрудничества.

Для эффективного сотрудничества нужна согласованность законов, поскольку многие страны в основу правового взаимодействия закладывают принцип обоюдного признания конкретного деяния преступлением, т.е. в юрисдикциях всех заинтересованных сторон данное правонарушение должно быть наказуемым. Когда в определенной юрисдикции отсутствует законодательство по киберпреступлениям, или оно плохо применяется, страна может превратиться в убежище для киберпреступников. С такими различиями можно справиться только совместными усилиями по гармонизации законов и усилению сотрудничества.

Сотрудничеству правоохранительных агентств по борьбе с киберпреступностью мешает не только нехватка подготовленных сотрудников и финансовых ресурсов; оно затруднено в силу того, что киберпреступлениями все еще занимаются обычные отделения полиции. У них нет необходимых знаний, оперативности, четкой технологии и политики реагирования на киберпреступления. Реализации эффективных решений препятствуют недостаток киберкриминалистов, многочисленные барьеры для сотрудничества, устаревшие или отсутствующие правовые механизмы, слабое международное взаимодействие и культурные парадигмы отдельных организаций.

Ответ на криминальную деятельность в физическом мире сложно повторить в киберпространстве. Этот факт лишний раз подчеркивает необходимость серьезной гармонизации законов в сфере киберпреступности и установления серьезных наказаний. Даже дела с бесспорными доказательствами не заканчивались заключением виновных под стражу. Одним из важных результатов очень немногих успешных дел является беспрецедентная демонстрация многостороннего международного сотрудничества правоохранительных агентств, обмена информацией и техникой сбора доказательств, установления личности нарушителей и их ареста. Тем не менее, такой уровень сотрудничества является скорее исключением, чем правилом.

Отмеченные недостатки способствуют тому, что жертвы киберпреступлений не верят в то, что правоохранительным органам удастся установить преступ-

Вызовы правоохранительным органам

- ✓ Несмотря на то, что интернет-преступность имеет международный характер, законодательство в сфере киберпреступности различно в разных странах.
- ✓ Даже в развитых странах эволюция угроз далеко превосходит необходимые адаптации уголовного кодекса и других основных законов.
- ✓ Киберпреступность часто носит международный характер: например, сайты детской порнографии могут быть зарегистрированы в стране А, разрабатываться в стране Б, а хозяин этого сайта и управление им находятся в стане В. То же относится к разработке и использованию вредоносного ПО.
- ✓ Страна, согласно международным законам, не несет ответственности за кибератакивность своих граждан, даже если эта деятельность *де факто* является актом войны по отношению к другому государству. В такой ситуации страны с киберамбициями могут прятать свою кибератакивность под прикрытием предположительно анонимных хакеров и хактивистов.
- ✓ Злонамеренное использование компьютера может быть обнаружено нескоро, когда Трояны или другое ПО отсроченного действия активизируется. Его также может быть сложно обнаружить (например, если вредоносное ПО крадет по 5 центов от каждого перевода денег из страны А в страну Б).
- ✓ Некоторые из жертв киберпреступников могут не хотеть обращаться в полицию, например, банки, которые, возможно правильно, считают, что ущерб от озвучивания факта хищения может превзойти потери от самого преступления. На более серьезном уровне это создает ситуацию, при которой все увеличивающийся сектор экономики постепенно выходит из-под защиты закона и должен полагаться в своей защите на свои собственные средства и/или специализированные частные компании.
- ✓ В большинстве стран количество киберполицейских мало, их карьерные перспективы незначительны. Полиции трудно конкурировать в борьбе за лучших и самых талантливых сотрудников с частным сектором.
- ✓ Своими собственными силами полиция не может обнаружить большую часть киберпреступлений, но вынуждена рассчитывать в обнаружении и преследовании за такие преступления на частные компании, например, интернет-провайдеров, операторов мобильной связи и других специализированных агентов. Доступные полиции средства не позволяют ей гарантировать безопасность гражданам в этой наиболее динамично развивающейся сфере криминальной активности.
- ✓ Такое положение вещей приводит к тому, что полиция больше не несет ответственности за кибербезопасность. А там, где нет ответственности, нет и обязательств. Что, в свою очередь, еще больше усложняет создание эффективных стратегий кибербезопасности.

ников.[11] В первую очередь, пострадавшие от киберпреступления обращаются в местное отделение полиции, которое, как правило, не имеет всего необходимого оборудования для расследования дела и не чувствует свою ответственность за раскрытие преступления. Вину, как правило, перекладывают на интернет-провайдера, платежную систему или вебсайт, на котором возникла

[11] Russell G. Smith, "Investigating Cybercrime: Barriers and Solutions," Association of Certified Fraud Examiners, Pacific Rim Fraud Conference, Sydney, 11 September 2003, p. 2.

проблема, возлагая ответственность на самого пострадавшего. Сравнивая большое количество киберпреступлений с небольшим количеством успешных расследований, пострадавшие не видят смысла сообщать о преступлении. Более того, автоматизация позволяет киберпреступникам реализовать стратегии получения крупных прибылей от большого числа незначительных атак. И за очень редким исключением, жертвы предпочитают не проходить через очень длительную процедуру дачи показаний.[12]

Одной из самых больших проблем правоохранительных органов является привлечение и удержание персонала, высококвалифицированного в области кибербезопасности и киберкриминалистики. Государственная служба остается малопривлекательной, так как не может конкурировать по зарплатам, карьерным перспективам и возможностям повышения квалификации, которые может предложить частный сектор. Правительству необходима стратегия по увеличению, улучшению, подготовке и удержанию высококвалифицированных специалистов в области информационных технологий.

Тогда как многие правоохранительные агентства технически оснащены и готовы расследовать он-лайн и киберпреступления, они сталкиваются с недостаточной поддержкой со стороны прокуратуры, судей и политиков. Правоохранительным органам требуется большая поддержка от этих участников, также как и от систем эффективного международного сотрудничества.

2.2.5. Судьи и прокуроры

Если правоохранительные органы многих стран смогли улучшить деятельность по расследованию киберпреступлений, сбор электронных доказательств, то работа судей и прокуроров в этом направлении оставляет желать лучшего. Опыт показывает, что в большинстве случаев судьи и прокуроры испытывают сложности при столкновении с новыми реалиями кибермира. От судей и прокуроров, следовательно, требуются особые усилия – подготовка, специализация и обмен опытом, позволяющие готовить обвинение и вести процесс по киберпреступлениям, а также должным образом использовать электронные доказательства.

Опыт частного сектора в области новых технологий был использован при проведении тренингов для правоохранительных органов. Он также может быть полезен и при подготовке судей. Тем не менее, этот потенциал пока еще остается не востребованным. В то же время, независимость и непредвзятость судей должна быть сохранена. Все судьи, следователи и прокуроры должны обладать базовыми знаниями о вопросах, связанных с киберпреступлениями и электронными доказательствами. Они должны разбираться в компьютерах и сетях, в вопросах использования информации и коммуникационных технологий в преступной деятельности; они должны знать внутреннее законодательство и международные стандарты, юрисдикции и территориальные границы, а также технические процедуры и правовые аспекты получения электронных доказательств. В результате таких тренингов судьи и прокуроры должны по-

---

[12] Serious Organised Crime Agency (SOCA); “International crackdown on mass marketing fraud revealed,” *Information Daily*, 4 October 2007, www.theinformationdaily.com/2007/10/04/international-crackdown-on-mass-marketing-fraud-revealed.

Вызовы судьям и прокурорам

- ✓ Глобальная природа киберпреступлений усложняет процессы задержания и преследования киберпреступников.
- ✓ Законы о киберпреступлениях либо отсутствуют, либо несовременны – со множеством лазеек для правонарушителей; наказания за киберпреступления незначительны; существует много препятствий для следователей в поиске и изъятии доказательств, а также для сотрудничества со свидетелями.
- ✓ Существует острая необходимость в том, чтобы все страны приняли строгое и гармонизированное законодательство по киберпреступлениям.
- ✓ Судьям, прокурорам и правоохранительным органам часто не хватает знаний для эффективного расследования и привлечения преступников к суду. Необходимо усовершенствовать сферу подготовки и образования, только в этом случае можно быть уверенными в надлежащей квалификации сотрудников, которые обладают необходимыми знаниями, умениями и возможностями для борьбы с киберпреступностью и выстраивания сильных обвинений.
- ✓ Необходимо усилить международное сотрудничество в области обнаружения и ареста киберпреступников.
- ✓ К международному сотрудничеству необходимо привлечь правительства, интернет-провайдеров, поставщиков финансовых услуг, банки, агентов по финансовым операциям, операторов мобильной связи, экспертов по безопасности. И это сотрудничество должно поощряться.

лучить знания о том, как проводить уголовное расследование в рамках внутреннего законодательства, какие следственные процедуры применять, как оформлять ордер на поиск и изъятие компьютерных систем и электронных доказательств. Они должны уметь ускорять международное сотрудничество, допрашивать свидетелей и экспертов, предоставлять и подтверждать электронные доказательства. Тем не менее, базовых знаний иногда бывает недостаточно для ведения дела о киберпреступлении. Чтобы справиться с такими ситуациями, необходимы следователи и прокуроры, обладающие специфическими знаниями, которые могут расследовать, готовить обвинение и вести процесс по сложным делам о киберпреступлениях или оказать помощь другим прокурорам и судьям.

Промышленность должна сотрудничать с правоохранительными органами, судьями и прокурорами, способствуя разработке инструментов, необходимых для преследования киберпреступников. Интернет-провайдеры, банкиры, поставщики финансовых услуг, агенты по финансовым операциям, правоохранительные органы, судьи и прокуроры должны действовать совместно, чтобы обеспечить поиск киберпреступников, лучшее понимание их методов, а также своевременный сбор доказательств. Интернет-провайдеры, в частности, должны принимать активное участие в поиске решений, учитывая контроль и ответственность за интернет-трафик, который проходит через их системы.

Несмотря на то, что правонарушители все еще опережают законодателей, Евросоюз пытается ликвидировать отставание, так как киберпреступность все больше угрожает защите информации, которая принадлежит гражданам, промышленности и правительству. Действия на национальном уровне не привели

к успеху в борьбе с ростом банковского он-лайн мошенничества, фишинга аккаунтов социальных сетей, увеличения числа вредоносных вирусов и продаж незаконного порнографического контента. Члены Евросоюза в настоящее время признают необходимость сотрудничества как на Европейском, так и международном уровнях для решения означенных проблем.

Определенный прогресс был достигнут в области подготовки судей и прокуроров. В июле 2007 года Европолом на базе Центра по борьбе с киберпреступностью была создана группа по вопросам гармонизации и проведению тренингов, главной задачей которой является координация усилий стран Евросоюза по подготовке сотрудников в сфере противодействия преступлениям с применением высоких технологий. Это позволит разработать единую Европейскую программу подготовки следователей и распространить полученный опыт за пределами Евросоюза. Партнерами проекта являются Европейская комиссия, Европейское бюро по борьбе с мошенничеством (OLAF), Евроюст, Европейский полицейский колледж CEPOL, Интерпол, Совет Европы, ООН, Центр расследований киберпреступлений в Университетском колледже Дублина – ведущий европейский центр исследований и образования в области киберпреступлений и цифровой криминалистики, университет Труа, Христианский университет в Кентербери, Болонский университет, а также частный сектор. 27 апреля государства-участники обратились к Комиссии с просьбой рассмотреть возможность создания специального агентства по борьбе с киберпреступностью, «чтобы оценить и изучить превентивные меры и следственные процедуры», которые должны выполнять государства-участники.[13]

2.2.6. Конечный пользователь

Тем, кто использует информационные технологии, необходимы осознание вопроса и соответствующее образование. Все пользователи, включая потребителей, малый бизнес, детей, школы и сотрудников компаний, должны не только осознавать риски киберпреступлений, но и владеть наилучшими способами самозащиты. Необходимо проведение образовательных кампаний, привлекающих внимание к вопросу, следует разработать программу обучения кибербезопасности, которая будет использована не только в школах, но и различными молодежными организациями, ассоциациями по предотвращению преступлений, группами по защите прав потребителей и добровольными местными организациями.

Будущим преступникам необходимо понимать, что они действительно рискуют быть пойманными, совершение киберпреступления так же серьезно, как и «физического» преступления. Рекламодатели тоже должны быть уверены, что их законные расходы на рекламу не становятся источником финансирования какой-либо незаконной деятельности. Работа должна быть продолжена и с торговыми агентами в направлении безопасности и сохранности их активов – баз данных и бизнеса.

---

[13] Council of the European Union, Council conclusion concerning an Action Plan to implement the concerted strategy to combat cyber-crime, 3010th General Affairs Council meeting, Luxembourg, 26 April 2010.

Общественности необходимо осознать, что результатом атаки на важные объекты инфраструктуры может стать гибель людей, угроза общественной безопасности; кибератаки способны влиять на национальную безопасность, могут привести к масштабному экономическому хаосу и разрушительным экологическим катастрофам. Необходимы более активные действия, подвигающие людей сообщать правоохранительным органам обо всех случаях электронных вмешательств и связанных с ними потерях. Таким образом, общественность может помочь правоохранительным органам получить необходимые знания, умения и возможности для борьбы с киберпреступлениями, а также способствовать совершенствованию законов, нацеленных на должное наказание преступников.

2.2.7. Частный сектор

Если реакцию правительства на киберпреступления можно охарактеризовать как ситуативную, реакцию частного сектора можно назвать бессистемной. Существует три традиционных ответа на подобные проблемы рынка: регулирование, налогообложение и страхование. Определить стоимость страховки невозможно, так как нет ни стандартных процедур, ни методики определения суммы ответственности за невыполнение стандартных процедур.

В киберпространстве отсутствует и то, и другое. Не существует ни общепринятых стандартов кибербезопасности, ни общепринятой системы ответственности за несоответствие таким стандартам. В такой ситуации страховые агентства задаются вопросом: как страховать риск? И ответ возможен только когда тот, кто принимает на себя риск, мотивирован его застраховать, в первую очередь, своей ответственностью. Но такой системы не существует.

Создание стимулов для обеспечения частным сектором безопасности киберпространства остается проблемой. По ряду причин компании частного сектора не хотят публично признавать существование проблем с безопасностью и также не хотят сами разрабатывать стандарты, которые приведут к возникновению ответственности там, где ее не существует. Если правительство не начнет разрабатывать стандарты, обязательные для частного сектора, то они никогда не будут созданы. Но сама идея разработки стандартов правительством имеет ряд недостатков. Возможна альтернатива – формирование обратной парадигмы: вместо того, чтобы правительство разрабатывало стандарты, нарушение которых предполагает наказание, следует совместно правительству и частному сектору разработать рекомендации по обеспечению кибербезопасности. Если это будет сделано, возможно, возникнет независимая сертификационная отрасль, и страховые взносы будут зависеть от соответствия разработанным стандартам. Еще одна, хотя и менее эффективная, альтернатива – государство само «дает добро» и сертифицирует соответствие стандартам. В любом случае, если стандарты будут разработаны, тогда и появится возможность страхования риска нарушения этих стандартов.

Более серьезным шагом будет переход от рекомендательных стандартов к традиционной регуляторной модели обязательных к исполнению стандартов. Этот шаг снова поднимет вопрос о том, как сделать действенными регуляторные распоряжения в сложной технической сфере. Тем не менее, возможен и другой вариант событий – применение регуляторной модели без создания

стандартов. Все, что правительству необходимо сделать, – определить желаемый результат (например, сокращение числа нарушений или вмешательств) и наказание за невыполнение постановлений. Обозначение последствий также создает ответственность (а, следовательно, и страховой риск) даже в условиях отсутствий стандартов достижения желаемого результата. Пока желаемый результат не является невозможным (например, отсутствие вмешательств), частный сектор может определить наиболее экономически эффективные способы достижения цели. Но реальных стимулов, подвигающих частный сектор к подобной деятельности, до сих пор не существует.

Еще одним возможным стимулом для частного сектора со стороны государства является налогообложение. Облагая налогом конечный продукт или предлагая налоговые кредиты/льготы на расходы, можно создать финансовый стимул. Хотя эти действия также могут привести к нежелательным последствиям, налогообложение остается инструментом, к помощи которого государства часто прибегают, чтобы воздействовать на частный сектор. В таком случае, например, парламент может рассмотреть вопрос о налоговом кредите на системы обеспечения безопасности как способе подтолкнуть частный бизнес к более серьезному отношению к кибербезопасности. Проблема состоит в необходимости продемонстрировать на правительственном уровне способность создавать правильные стимулы. Частные компании, особенно работающие в киберпространстве, сильно не доверяют вмешательству и инструкциям правительства, и потребуются значительные усилия и политическая воля для создания культуры, которая рассматривает гражданское право как основу реформирования сектора безопасности.

2.2.8. ИТ-сектор

Сектор информационных технологий является ключевым в решении проблем обеспечения кибербезопасности, именно этот сектор в ситуации увеличивающегося числа киберугроз и кибератак может постепенно стать базовым элементом стратегии национальной обороны, постепенно вытеснив традиционный сектор безопасности. Подобное положение вещей может привести к ряду проблем, в особенности для самой ИТ-отрасли – как сохранить независимость, свободомыслие и инновационность, играя главную роль в вопросах национальной обороны?

В ближайшее же время необходимо добиться помощи от сектора информационных технологий – нужны технологические решения, которые бы на шаг опережали угрозы. Необходимо сотрудничество в сфере ускоренной разработки межоперационных продуктов безопасности, упрощения интеграции этих продуктов в сложные потребительские системы, что имеет конечной целью одновременное обеспечение безопасности сетей и доступа к важнейшим объектам.

Качество программного обеспечения также нуждается в улучшении. Много внимания уделялось безопасности операционных систем, но в настоящее время акцент сместился на уровень приложений, безопасностью которых практически не занимались. Кроме приложений, целью атак могут стать программы более низкого уровня, например, встроенные. Снижению уязвимости в

этой области практически не уделялось внимания, и эту ситуацию необходимо изменить.

Инструменты безопасности должны стать проще или быть встроенными. Чем сложнее инструмент безопасности, тем меньше людей будут им пользоваться. Полагаться на конечного пользователя в плане обеспечения его/ее личной ответственности за безопасность компьютера или мобильного устройства – то же самое, что просить водителя купить ремни или подушку безопасности в качестве «дополнительного» средства защиты в случае аварии. Возможно, компании частного сектора должны нести некоторую ответственность за ущерб, причиненный незащищенными услугами или продуктами.

Регистрация доменов в Интернете должна быть защищена от мошенников. В сфере защиты объектов важнейшей инфраструктуры необходим более активный диалог между производителями решений и пользователями. Такой подход обеспечит принятие правильных решений, доступность сетей и возможность учитывать даже в коммерческих продуктах особые требования.[14]

Технологическим компаниям необходимо стать партнерами; бизнес, наука, правительства и исследовательские центры должны понимать новые угрозы и извлекать пользу из новейших разработок ученых. Должно поощряться сотрудничество пользователей, правоохранительных органов, интернет-провайдеров, банков, операторов мобильной связи и других участников в области исследований.

2.2.9. Банки и финансовые учреждения

За последние два десятилетия объем и количество финансовых услуг значительно возросли, а использование электронных средств ведения бизнеса как он-лайн, так и при помощи удаленного доступа, стало широко распространенным явлением. С середины 1990-х годов инвестиции в банковские технологии сосредоточились, в основном, в сферах он-лайн банкинга, брокерских и страховых услуг, с целью сделать их более удобными, качественными и дешевыми. Развивающиеся рынки все больше используют новые методы электронных платежей и беспроводные технологии электронных финансов. Но с преимуществами новых технологий также пришли новые опасные риски – как системные, так и мошенничества, кражи, вымогательства, ухудшение кредитоспособности. Финансовые услуги, и платежные системы в частности, являются одной из наиболее важных областей национальной инфраструктуры. Система платежей, пострадавшая от несанкционированного доступа или атаки хакеров, может представлять серьезную угрозу для всей экономики. Общественное благосостояние потенциально находится под угрозой, если бизнес и торговля не могут обеспечить минимальные стандарты электронной безопасности.

Основная проблема деятельности банков, финансовых учреждений и некоторых других частных предприятий состоит в их нежелании сообщать в правоохранительные органы об электронных проникновениях. Эти структуры часто предпочитают сохранять молчание и самостоятельно справляться с последствиями атак и вмешательств, даже если они значительны. Существует пять причин, по которым банки и финансовые учреждения не хотят сообщать в

---

[14] McAfee, *Multipoint Strategy to Fight Cybercrime*, 30 November 2009.

правоохранительные органы о вмешательствах и потерях: 1) нежелательная огласка, которая может привести к колебанию цены их акций, ухудшить позиции на рынке, подорвать доверие общественности и клиентов, создать проблемы с капитальными инвестициями; 2) конкуренты могут использовать негативную информацию для того, чтобы получить преимущество: например, переманить клиентов; 3) необходимость защиты тайны клиента; 4) риск оказаться втянутым в длительный и дорогостоящий судебный процесс; 5) страх сотрудников отделов информационных технологий быть уволенными в случае сообщения об инцидентах. Кроме того, возможно и отсутствие доверия к правоохранительным органам или опасения, что это может привести к ужесточению правил в отрасли или во всей сфере электронного бизнеса.

Терпимость к такому поведению еще более усложняет ситуацию. Если правительство не может заставить банки и финансовые учреждения сообщать о вмешательствах и потерях, оно лишает государство монополии на применение силы для установления верховенства права. Это также окажет непосредственное влияние на другую важную обязанность банков и финансовых учреждений – предотвращение отмывания денег и информирование об этом. Правительство и другие органы власти, занимающиеся борьбой с киберпреступлениями, должны обязать всех пострадавших от киберпреступлений сообщать о них. Доступ к более полной информации о реальной картине киберпреступлений также позволит правоохранительным органам эффективнее привлекать к ответственности преступников, сдерживать потенциальные атаки, приводить в исполнение более эффективные законы.

2.2.10. Объекты инфраструктуры особой важности

Защита важнейших национальных объектов и служб во все более сложном и непредсказуемом взаимосвязанном мире становится достаточно сложной задачей. Национальная оборона, общественная безопасность, экономика и качество жизни людей уже давно зависят от эффективного предоставления ряда важнейших услуг, среди которых телекоммуникации, энергетика, банковские и финансовые услуги, транспорт и жизненно важные: поставки воды и продовольствия, чрезвычайные службы. Эти услуги национального значения известны как «важнейшая национальная инфраструктура» (ВНИ).

Быстрый рост и интеграция мировой телекоммуникационной инфраструктуры, базирующейся преимущественно на Интернете, связали объекты важнейшей инфраструктуры так, как это ранее невозможно даже было себе представить. Определение взаимосвязей стало сложной и трудной для понимания задачей, особенно когда объекты важнейшей инфраструктуры разбросаны по государственному и частному сектору.

Решение проблем обеспечения кибербезопасности требует скоординированных действий, что связывает между собой внутреннюю, внешнюю и оборонную политику. Евросоюз считает, что уникальный многомерный подход к безопасности ОБСЕ может стать прекрасной основой для таких решений. Но до сих пор единой точки зрения по этому вопросу или выработанного подхода нет и внутри самого Евросоюза. Тот факт, что в Европе отрасли ВНИ, такие как энергетика, телекоммуникации, транспорт и вода, все более становятся взаи-

Вызовы банкам

- ✓ Финансово мотивированная киберпреступность находится на подъеме в связи с тем, что по всему миру каждую секунду осуществляются электронные переводы значительных сумм.
- ✓ Ситуация становится еще более привлекательной для преступников, так как банки не хотят сообщать об атаках.
- ✓ От компьютерных «краж со взломом» нет страховки (нет достаточно крупного сообщества пострадавших, чтобы такие страховки стали выгодными и, что не менее важно, их можно было бы рассчитать).
- ✓ В большинстве стран нет специальных отделов полиции по киберпреступлениям. Более того, отделы полиции по киберпреступлениям во всем мире, как правило, специализируются на определенных преступлениях (таких как педофилия и контрабанда людьми).
- ✓ Банки страдают не только от краж со взломом, но и от целого ряда атак: от попыток получить данные клиента до отмывания денег.
- ✓ Потенциальные цели киберпреступников, атакующих центральные банки, весьма разнообразны: получение доступа к различным секретным данным – от решений по процентным ставкам до планов интервенции на валютных рынках.
- ✓ Сталкиваясь с этой новой реальностью, банковский сектор все больше полагается на свои силы в защите – как на собственные внутренние ресурсы, так и на дорогую и очень избирательную помощь извне.
- ✓ Общей тенденцией банковского сектора является растущее недоверие к возможностям сил правопорядка в предоставлении помощи. Это экстраординарная ситуация, так как в некоторых странах на долю банковского сектора приходится значительный процент ВНП, и во всех странах именно он – источник жизненной силы экономики.
- ✓ Такая ситуация бесперспективна. Если банки не могут рассчитывать на то, что их электронные системы должным образом будут защищены государством и международным сообществом, тогда финансовый сектор перейдет к высоко секретным внутренним сетям – шаг, который будет иметь очень серьезные последствия для мировой экономики в условиях глобализации.

мозависимыми, создает новые сложности и увеличивает риски серьезных нарушений в работе.

В настоящее время еще не разработано понимание пан-европейской ВНИ, которая бы учитывала географические и другие особые для каждого сектора взаимосвязи и взаимозависимости. Изучение этой сложной инфраструктуры требует совместных междисциплинарных усилий исследователей, представителей промышленности и правительственных организаций. Эти исследования зависят от применения моделей и симуляторов, так как, по очевидным причинам, аварии и способы ликвидации их последствий не могут изучаться или проверяться в реальных условиях.[15]

[15] См: DIESIS: Design of an Interoperable European federated Simulation network for critical InfraStructures, Fraunhofer IAIS, доступно на: www.iais.fraunhofer.de/4819.html?&L=1 и www.diesis-project.eu.

Вызовы в сфере защиты важнейших объектов национальной инфраструктуры

- ✓ Функционирование экономических, финансовых, правительственных, общественных объектов и объектов здравоохранения в настоящее время зависит от киберпространства. Значит, они уязвимы и являются привлекательными целями.
- ✓ Защита ВНИ стала приоритетом для большинства стран. Однако понимание важности еще не означает наличие эффективных механизмов обеспечения защиты.
- ✓ Сегодня каждый сектор общественной и частной жизни является потенциальной целью кибератак – и даже более того, целью секретных разведывательных операций и саботажа со стороны иностранных держав. Государство, в большинстве случаев, не может обеспечить надежную защиту от этих атак.
- ✓ Чтобы обеспечить реальное сотрудничество общественных институтов и частного сектора в защите ВНИ, частный сектор должен увидеть преимущества сотрудничества с правоохранительными органами, а затем совместно разработать систему защиты. На данный момент этого не происходит.
- ✓ Подобное положение вещей делает атаки на объекты ВНИ, находящиеся в частных руках, особенно привлекательным: банковским грабителям, террористам и иностранным державам легче использовать свои возможности ведения кибервойны.
- ✓ Некоторые объекты имеют особое значение: главные аэропорты, системы управления воздушным движением, основные узлы линий электропередач, химические предприятия и система международных финансов. Эти потенциальные цели знают о своей уязвимости, но предпочитают разрабатывать собственные системы кибербезопасности. Ситуация, в которой наиболее важные и наиболее вероятные цели вынуждены сами о себе заботиться, более неприемлема.
- ✓ Проблема усложняется тем, что как показывает практика, вредоносное ПО уже заносилось в системы объектов ВНИ. Еще требует своего осознания связанная с этим необходимость разработки разумных систем, способных автоматически и регулярно проверять себя на наличие новейшего вредоносного ПО. Эти системы достаточно дорогостоящи, в случае же их неправильного использования возможно снижение для всей системы взаимосвязанных ВНИ положительного эффекта определенных контрмер.
- ✓ В этой области необходим единый гармонизированный подход со стороны всех участников, прогресс в этой сфере невозможен без международного сотрудничества.

Первый призыв к сотрудничеству государств-участников в области защиты ВНИ прозвучал после терактов в Мадриде, которые продемонстрировали проблемы с обменом информацией относительно угроз объектам ВНИ. В настоящее время Еврокомиссия рассматривает предложения, согласно которым страны ЕС должны будут определить все компоненты своей ВНИ и проводить периодические проверки безопасности. Результаты этих проверок будут обобщаться центральным координационным органом ЕС, который, в свою очередь, определит стандарты и проведет мониторинг их выполнения.

Тем не менее, попытки провести стандартизацию в ЕС могут столкнуться с рядом проблем. В ЕС 27 государств, каждое из которых имеет свое определение ВНИ, разные степени рисков и разные военные, технические и политические ресурсы противодействия рискам. Следовательно, общеевропейский подход, возможно, потребует такой степени сотрудничества и обмена информацией, которая неприемлема для тех государств, которые не видят в данный момент необходимости в предоставлении такой важной информации.

2.2.11. Викиликс

22 октября 2010 года мировой он-лайн «информатор» WikiLeaks.org (согласно веб-сайту «некоммерческая медиа-организация, задачей которой является сообщение общественности важнейшей информации и новостей»), опубликовала 391 832 секретных доклада, касавшихся войн а Ираке и Афганистане за период с 2004 по 2009 годы – War Logs (полевые журналы). Эти документы – в основном оригиналы донесений с поля боя американских военных, большая часть из которых – 97 % являются секретными. За несколько недель до их формальной публикации Викиликс передал документы для анализа некоторым службам новостей – среди них были «Нью-Йорк таймс», «Шпигель», «Гардиан» и «Аль-Джазира», и все эти службы опубликовали специальные репортажи. Пентагон осудил публикации, расценив их как преступление. Также Пентагон потребовал возврата украденной собственности и предупредил, что опубликование документов может привести к ухудшению ситуации в Ираке, а также к риску для жизни американских солдат, так как террористы изучают документы, чтобы получить оперативную информацию, необходимую для планирования своих атак.

В документах содержалось очень незначительное количество действительно секретной информации, что было отмечено СМИ после серьезного изучения документов, где содержалась информация, которая была давно и широко известна: что правительство Ирака применяло пытки по отношению к своим гражданам; что в Ираке действовали батальоны смерти; что правительство Ирана финансировало боевиков-шиитов. Ничто из этого не было новостью. В докладах сообщалось о том, с чем пришлось столкнуться подразделениям – например, случаи применения самодельных взрывных устройств (СВУ), засады, убитые гражданские, случаи дружественного огня, ДТП и так далее. В большей части в докладах содержалась первичная информация, а не разведданные. Там также не было информации, полученной в процессе сбора разведданных, следовательно, не раскрывались источники и методы. И хотя материал часто сравнивают с публикацией в 1971 году документов Пентагона Даниелем Эллсбергом, сходства здесь мало. Эллсберг предоставил СМИ совершенно секретный аналитический доклад о Вьетнамской войне, подготовленный для Министерства обороны, а не оригинальные документы с поля боя. Бумаги Пентагона продемонстрировали ложь правительства относительно войны, и их публикация была способом привлечь к этой ситуации внимание общественности.

В то же время 28 ноября 2010 года Викиликс объявил о публикации 251 287 депеш посольств США, назвав это «наибольшим массивом конфиденциальных документов, который когда-либо был предан публичной огласке». Веб-сайт заявил, что эта публикация приведет к беспрецедентному исследованию

внешней политики США. На первый взгляд, складывается впечатление, будто сбылись мечты исследователей. Журналисты отделов новостей «Нью-Йорк таймс», «Гардиан», «Шпигеля», «Ель Паис» и «Ле Монд», изучая богатейшую коллекцию «примеров дипломатической конфиденциальности», «ограниченной честности в политике», а также тайных соглашений, опубликовали часть из полученных ими документов и обещают опубликовать остальные постепенно в течение следующих месяцев по мере проявления интереса к ним со стороны других агентств новостей. Как и в случае с War Logs, эти дипломатические депеши были получены из системы секретного протокола маршрутизатора Сети (СПМС, SIPRNet), которой пользуется правительство США. Эта система используется для передачи как информации с ограниченным доступом, так и информации с грифом *секретно* включительно. Большие партии документов были переданы солдатом, рядовым первого класса Брэдли Меннингом, который был арестован в мае 2010 года в Ираке Управлением уголовных расследований армии США и обвинен в похищении большого количества секретных документов и передаче их посторонним лицам. Меннинг знал, что информация, которую загружал, была секретной и не подлежала распространению. Также он знал, что его действия незаконны, могут спровоцировать неприятности и последующее привлечение к ответственности. Правила, определяющие степени секретности информации в США, изложены в Указе Президента № 13526. Согласно этому Указу, секретная информация отнесена ко второй наивысшей степени секретности, обнародование такой информации может нанести серьезный ущерб национальной безопасности США.

Называя эту утечку «cablegate», Викиликс заявляет, что обнародованные документы доставят много неприятностей правительству США, но содержат они открытую информацию, которую граждане США и мировая общественность имеют право знать. «Обнародованные документы раскрывают противоречие между публичным образом США и тем, что делается за закрытыми дверями, и акцентируют следующее положение: если граждане в демократической стране хотят, чтобы правительства выполняли их волю, они должны видеть, что происходит за сценой». Та информация, что в настоящее время циркулирует в Интернете, прессе и на телевидении, является фактом серьезного нарушения доверия. Некоторые из депеш дискредитируют мировых лидеров; в других разглашаются секретные планы НАТО относительно войны США против России из-за Балтийских государств в случае какого-либо вмешательства со стороны России. Некоторые, наиболее взрывоопасные из опубликованных депеш, касаются арабских лидеров стран Персидского залива и их просьб к США принять меры в ответ на возможную ядерную программу Ирана. В депешах из Исламабада сообщается, что правительство Пакистана опять затягивает с выполнением достигнутого два года назад соглашения, позволяющего США переместить обогащенный уран (который был предоставлен США в 1960-х годах в рамках программы мирного атома). Пакистанская сторона высказывала опасения, что если соглашение станет достоянием гласности, у народа и СМИ создастся впечатление о планах США взять под контроль ядерное оружие. В другой депеше передавались слова главы Комитета начальников штабов армии США, сказанные послу США, суть которых сводилась к следующему: пусть и с неохотой, но глава Комитета может заставить Президента Зардари подать в

Будущие вызовы: Викиликс

- ✓ Викиликс очень эффектно опубликовал секретные материалы. Тем самым он привлек к себе общественное внимание. В этом нет ничего нового. Сразу же вспоминаются «Бумаги Пентагона».
- ✓ Новым, во-первых, является количество просочившихся документов (где-то более 640 000). Во-вторых, обнародованием документов занимался не один человек, который раскрыл кому-то постороннему возможно большое, но все же, незначительное количество документов (агент КГБ, который выдал секретную информацию; недовольный сотрудник банка, продавший третьей стороне диск с конфиденциальными данными клиентов; недовольный чиновник, сообщивший СМИ «горячую» информацию). Случай Викиликс отличен: это открытая для всех интернет-платформа, задачей которой является разглашение частной/секретной информации. Викиликс – это приглашение для всех разглашать любую информацию, которая вызывает беспокойство. Формат предполагает размещение информации любого плана – от стратегической до конфиденциальных личных данных и обычных для интернет-папарацци материалов.
- ✓ В конечном итоге, для формата Викиликс нет ни границ, ни ограничений. Хорошо срежиссированный запуск платформы (изначальное предоставление более 390 тысяч военных докладов, за которыми последовали публикации дипломатических документов, и все это получило обширное освещение во всех мировых СМИ) привлек всех, особенно идеалистов и недовольных – любой грязный секрет должен быть представлен на суд общественности, показывая людям, что ничто не является секретом и ничто больше нельзя скрыть. Викиликс нужно понимать как приглашение к уничтожению любой секретности и любой личной тайны.
- ✓ Суть Викиликс, однако, состоит не только в этом. С одной стороны, были заранее установлены связи с влиятельными СМИ (от «Шпигель он-лайн» до «Нью-Йорк таймс»), которые гарантировали, что журналисты просеют тонны разглашенных документов в поисках действительно пикантных подробностей. Следовательно, Викиликс – коммерческое предприятие. С другой стороны, Викиликс открыто апеллировал к анархическому, протодемократическому сегменту Интернета и рассчитывал на его реакцию. Таким образом, совмещались коммерческие и анархические цели проекта.
- ✓ К подобному повороту событий никто не был готов – и не готов в настоящее время. Феномен Викиликс вызывает огромное количество вопросов. В первую очередь, очевиден вопрос о праве общественности знать и о праве на тайну. Есть, кроме того, значительно более конкретные вопросы: как защитить правительства (или любого участника Интернета) от массивных утечек, которые происходят при помощи недовольных сотрудников или других людей (например, супруг, с которым разводятся)? Как защитить – даже на частном уровне (от Фейсбука до плохо защищенных смартфонов и персональных компьютеров) – конфиденциальную, личную и частную информацию? Как совместными усилиями решить проблему на национальном уровне? И поскольку этот уровень явно недостаточен в эпоху глобального Интернета, возникает еще вопрос: какие международные действия необходимы и применимы?
- ✓ Вопрос очень актуален: если убедительные и полные ответы не будут найдены, анархическая реакция на спектакль «Викиликс» перейдет в постоянное и опасное явление. Это существенно подстегнет «балканизацию» Интернета на большое количество надежно защищенных внутренних сетей. Последствия будут непредсказуемы.

отставку и даже покинуть страну. Естественно, Америка и ее союзники оказались в замешательстве.

По словам Генерального прокурора США, американское правительство планирует привлечь «Викиликс» к уголовной ответственности, поскольку ресурс обнародовал секретные документы Государственного департамента США, что поставило под угрозу безопасности нации. Пентагон ужесточает допуск к информации, включая ограничения на применение устройств хранения информации, таких как оптические диски и флеш-накопители. Но нет сомнений, что правительство США несет ответственность за фиаско с «Викиликс» – небрежность в защите конфиденциальных донесений своих послов. В то же время Хилари Клинтон и другие официальные лица прилагают максимум усилий, чтобы принести извинения мировым лидерам и послам и, по возможности, избежать негативных последствий.

Сайт WikiLeaks.org был закрыт хостинговой компанией, управляемой корпорацией «Амазон», но действия представителей крупного бизнеса направленные на то, чтобы заставить веб-сайт замолчать, привели к большому количеству ответных он-лайн атак со стороны активистов за свободу слова – атак, от которые пострадали операторы безопасных электронных платежей Мастеркард (Mastercard) и Виза (Visa). Кажется, что безопасность обеспечения доступа к бизнес-данным еще некоторое время будет в центре внимания, в то же время так называемые «хактивисты» объявили, что другие сайты пострадают от DDos-атак. PayPal (система электронных платежей) пострадала от серьезной атаки с применением вредоносного ПО, после того как были заблокированы он-лайн переводы для «Викиликс». Это поднимает новую проблему: сотрудничество интернет-провайдеров и правительства – это иное название цензуры или именование ответственности бизнеса в борьбе с анархией и беззаконием всемирной паутины?

2.3. Реагирование: сотрудничество общественных институтов и частного сектора

Примеры не налагающего взаимных обязательств сотрудничества общественных институтов и частного сектора под эгидой Международного союза электросвязи:

МСЭ, появившийся в результате Международного саммита информационного общества (МСИО), проходившего в Женеве в 2003 году, должен возглавить координацию международных усилий по обеспечению кибербезопасности. МСЭ был назван организацией, ответственной за реализацию Линии действий С5 Женевского Плана действий МСИО: «Построение доверия и безопасности при использовании ИКТ». МСЭ запустил многостороннюю Глобальную программу кибербезопасности (ГПК), в рамках которой действует инициатива по он-лайн защите детей, также было налажено сотрудничество с Международным многосторонним партнерством против киберугроз (ИМПАКТ), Малайзия.

Основные задачи он-лайн защиты детей следующие: определение рисков для детей в киберпространстве; привлечение внимания к проблеме; разработка инструментов уменьшения рисков, а также обмен знаниями и опытом.[16]

---

16 ITU website 2010.

Цель ИМПАКТ – улучшение возможностей предупреждения, защиты и реагирования на киберпреступления.[17] Центр глобального реагирования ИМПАКТ создал Сетевую систему раннего предупреждения (NEWS) и электронную защищенную прикладную платформу сотрудничества для экспертов (ESCAPE) совместно с частным сектором и правительствами. ИМПАКТ также организовывает брифинги на высшем уровне, обмен мировым опытом, сертификацию и проверку безопасности объектов.

Так как большая часть сетей и важной инфраструктуры находится в руках частного сектора, партнерство правительства, корпораций и частных лиц, а также региональное и международное сотрудничество необходимы для обеспечения безопасности киберпространства. Пока что многие государства с трудом налаживают обеспечение кибербезопасности через сотрудничество общественных институтов и частного сектора (СОИЧС).

СОИЧС и вызовы обмена информацией

- ✓ Понятно, что частный сектор неохотно делится секретной служебной информацией о вмешательствах, реальном ущербе, кражах и преступлениях, также как и о практиках предупреждения, как с правительственными агентствами, так и с конкурентами, – потому что обмен информацией является рискованным предложением с неясными выгодами. Ни одна компания не хочет, чтобы информация, переданная конфиденциально, всплыла на поверхность, так как это может нанести урон их позиции на рынке, клиентской базе или капитальным инвестициям.
- ✓ Также частные компании не хотят рисковать, добровольно втягиваясь в длительные и дорогостоящие судебные процессы. Представители отрасли опасаются, что неизбежно в ходе расследования случится разглашение данных невиновных клиентов. Негативная известность или разглашение в результате сообщений о нарушении в информационной инфраструктуре могут поставить под угрозу доверие клиентов или инвесторов к продукту компании. Более того, компании боятся передачи коммерческих секретов конкурентам и, следовательно, не хотят разглашать служебную информацию. Они опасаются, что передача этой информации правительству может привести к усилению регуляторной политики в отрасли или в электронной торговле в целом.
- ✓ Кроме того, может существовать определенное недоверие к правоохранительным органам или опасения, что системы компании могут быть заблокированы на время следствия, из-за чего возникнут производственные потери либо отставание в разработках. По этой причине многие предприятия частного сектора, включая банки, считают лучшим для себя хранить молчание и терпеть убытки в результате компьютерных атак и вмешательств. Более того, немногие высокотехнологичные компании заинтересованы в том, чтобы клиенты воспринимали их как активных агентов правоохранительных органов. Правительственные агентства в то же время слишком часто требуют информацию от частного сектора, давая взамен очень мало. Таким образом, существует слишком много препятствий информированию о случаях кибервмешательств.

[17] ITU website 2010.

- ✓ Перспектива того, что конфиденциальная бизнес-информация, переданная правительству, может подлежать разглашению в соответствии с другими нормами, например, Законом о свободном доступе к информации, может стать труднопреодолимым препятствием для обмена информацией.
- ✓ С другой стороны, в частном секторе уже существуют механизмы обмена информацией, которые не требуют вмешательства правительства. Например, и «белые хакеры», и сообщество исследователей в области безопасности предоставляют ценную помощь частному сектору. Они активно обмениваются информацией, что позволяет предотвратить большое количество атак и определить слабые места до того, как причинен ущерб. В частном секторе обмен информацией о слабых местах и средствах восстановления информации происходит повседневно, особенно на техническом уровне. Этот процесс активирован не распоряжениями правительства. Скорее, импульс основан на хорошо зарекомендовавшем себя опыте обмена информацией между инженерами ведущих телекоммуникационных компаний по защите систем и сетей. Участие правительства в этом обмене будет приветствоваться только в том случае, если оно привнесет дополнительные выгоды в существующую практику.
- ✓ Существует острая необходимость в надежном, продуктивном и активном сотрудничестве правительства с частным сектором. Правительственные агентства должны уважать конфиденциальность так же, как и ценность информации и секретов, которые частный сектор может передать им для выполнения поставленных задач. Чтобы обе стороны выполнили свои задачи, необходима постоянная, в режиме реального времени, обратная связь по обмену информацией. Стороны, обеспечивающие ИТ-безопасность, будут участвовать в обмене информацией только в случае абсолютной уверенности, что эта информация защищена от разглашения. Следовательно, все партнеры должны принять в качестве необходимого предварительного условия меры по защите секретной информации. Только на такой основе будет возможно построить доверительные отношения и начать обмен информацией. Такие же принципы применимы и к обмену информацией между правительствами и международными организациями.

Три уникальных качества характеризуют партнерство в сфере кибербезопасности, что приводит к некоторым осложнениям: 1) вопросы собственности в киберпространстве – как интеллектуальной, так и материально измеримой, могут не иметь прямых параллелей с существующими концептами собственности, закрепленными в других соглашениях СОИЧС; 2) как правило, СОИЧС осуществляется на базе регуляторных структур, возникших вокруг местных, региональных, федеральных, международных и смешанных органов власти. Такого комплекса властей или регуляторных структур нет в киберпространстве. Кроме того, компании были и могут быть против идеи регулирования Интернета; 3) требуется значительно меньше времени для киберразработок, инцидентов, реагирования и выявления угроз, чем в традиционных областях СОИЧС.

Вопрос обмена информацией также имеет первостепенное значение. Можно предположить, что выявить новые киберугрозы и обменяться информацией по этому вопросу относительно просто. Но это не так. Не существует единого мнения, что подразумевать под обменом, и будет ли он действительно эффек-

тивным. Какой информацией следует правительству делиться с частным сектором, и что частный сектор должен сообщать правительству? Что это изменит? И как получатель будет использовать информацию?

Задача сотрудничества общественных институтов и частного сектора в области кибербезопасности, в широком понимании, – разработать приемлемые стандарты и методики (например, обнаружения аномальной активности и поведения), что в дальнейшем позволит уведомить и пользователей, и поставщиков о существовании слабых мест и характеристик процессов и технологий, провести их корректировку с целью минимизации либо предотвращения нарушения гарантированного доступа либо приватности пользователей.

Эффективность партнерства обусловлено тремя необходимыми для обеспечения кибербезопасности положениями: 1) распознавание: партнерство должно способствовать определению, обнаружению и отслеживанию вызывающего беспокойство поведения; 2) защита: партнерство должно обеспечить выполнение всех стандартов безопасности, призывая к ответственности тех, кто им не следует; и 3) реагирование: предоставление инструментов для проведения криминалистических экспертиз после сбоев, анализа слабых мест, выявления изъянов в системе безопасности и эффективного установления тех, кто произвел атаку. Тем не менее, эти действия, как и стимулы для более активного сотрудничества и санкции за невыполнение предписанных процедур, должны быть согласованы всеми сторонами – поставщиками, пользователями и правительством.

Другими компонентами, которые могут быть добавлены, являются: 1) инспекции и введение в действие стандартов для поставщиков и интернет-провайдеров; 2) возможность наблюдать за сетями, искать и определять будущие угрозы и предупреждать всех пользователей до того, как возникнет чрезвычайная ситуация; 3) возможность отвечать на атаки через предупреждения и технические изменения, а также планировать восстановление важнейших систем после чрезвычайных ситуаций; 4) необходимая защита частной жизни и свободы слова, прав человека и интересов бизнеса с учетом интересов правительства; и 5) механизмы международного сотрудничества в области обеспечения кибербезопасности.

Чтобы быть эффективной, модель СОИЧС в области обеспечения кибербезопасности должна представлять интересы всех сторон, чьи согласованные действия могут дать желаемый результат. Это означает, что партнеры должны: 1) играть важную роль или быть действительно заинтересованы в усилении безопасности киберпространства; 2) быть в состоянии показать, что преследуя свои интересы, они также стоят на страже интересов всего общества; и 3) количество партнеров должно быть относительно невелико, что даст возможность действовать эффективно, быстро и в то же время сохранять широкое представительство и способность влиять на действия всех партнеров.

В число участников должны входить: 1) поставщики – круг, который в зависимости от целей партнерства может быть так же широк, как и круг пользователей. В эту категорию должны входить поставщики контента, интернет-провайдеры, производители программного обеспечения и аппаратного оборудования, представители телекоммуникационных компаний и операторы мо-

бильной связи; 2) пользователи – не только отдельные лица, как принято считать, но и крупный и малый бизнес, организации, ассоциации, а также государственные учреждения, а также внутренние и иностранные пользователи; 3) правительство, которое призвано играть две важные и четко определенные роли. Во-первых, как защитник интересов общества правительство является регулятором рынка. Во-вторых, будучи крупным потребителем интернет-услуг, правительство сильно зависит от Интернета, так как применяет его для общения со своими гражданами и предоставления им услуг.

И наконец, необходимо помнить, что, с точки зрения частного сектора, участие в СОИЧС требует реальных затрат – от времени до утраты некоторых возможностей из-за прямого участия. На практике, немногие участники в промышленности/частном секторе выделяют своих штатных сотрудников для работы над такими проектами. Более того, участие предприятия в СОИЧС может привести к риску потери репутации торговой марки, непредвиденным расходам в юридической сфере, а также может стоить политического капитала, поскольку предприятие, принимающее участие в определенных акциях, может быть рассмотрено как сторонник СОИЧС.

2.4. Реагирование: международное сотрудничество

Так как все больше правительств признают кибербезопасность одним из приоритетов национальной безопасности, пришло время соглашений в сфере международного законодательства по вопросам кибербезопасности. «Министр Вооруженных сил Великобритании Ник Харви призвал правительства всего мира разработать законы, регулирующие использование киберпространства. По сообщению Би-Би-Си, выступая в Королевском институте международных отношений, он сказал, что вопросом времени остается систематическое использование террористами киберпространства не только в качестве средства коммуникации для своих собственных организаций, но и как метод атак. Правительство Великобритании пообещало выделить 650 миллионов фунтов стерлингов в течение следующих 4 лет на Национальную программу кибербезопасности, чтобы защитить граждан и национальную инфраструктуру от кибератак».[18]

США также недавно объявили кибербезопасность своим приоритетом, создав Кибернетическое командование США. «Принимая во внимание растущую зависимость от киберпространства, это новое командование объединит ресурсы департаментов по выявлению слабых мест и противодействию все большему спектру киберугроз для нашей военной системы», – объявил 21 мая 2010 года Министр обороны Роберт Гейтс.[19]

Недавние предложения России по договору о киберпреступлениях (хотя и отвергнутые ООН, в особенности Канадой, США и Евросоюзом) показывают, что предпринимается все больше попыток достичь единства в вопросах кибербезопасности, несмотря на то, что все еще есть проблемы в переговорах по вопросам гармонизации различных стандартов и правовых систем.

---

[18] ComputerWeekly.com, 10 November 2010.

[19] http://www.af.mil/news/story.asp?id=123205791.

Наверное, наиболее серьезным примером международных договоров по вопросам кибербезопасности является Конвенция Совета Европы о киберпреступлениях. Конвенция была ратифицирована тридцатью странами, включая США, и «ее главные задачи: 1) гармонизация элементов внутреннего законодательства, касающихся правонарушений и соответствующих положений в сфере киберпреступлений; 2) установление полномочий и процедур, необходимых для расследования и судебного преследования за такие правонарушения, а также за другие правонарушения, совершенные при помощи компьютерных систем; для сбора доказательств по уголовным преступлениям в электронной форме; 3) разработка механизмов быстрого и эффективного международного сотрудничества».[20] Конвенция также предусматривает налаживание сотрудничества подписавших ее сторон в проведении международных расследований и создание системы предупреждения о кибератаках, работающей в режиме «24/7». Принятая в прошлом году Стокгольмская программа Евросоюза предусматривает дальнейшие меры по улучшению борьбы с киберпреступлениями. Еврокомиссар по вопросам внутренней политики должен представить новую «стратегию безопасности», включая проект законодательства по улучшению защиты от атак на сети и информационные системы.

Также как НАТО и другие организации, в последнее время Евросоюз проявляет все больше активности в вопросах обеспечения кибербезопасности, включая создание ENISA (Европейского агентства сетевой и информационной безопасности), задачей которого является обеспечение высокого уровня сетевой и информационной безопасности в странах Евросоюза. Более того, в 2006 году Евросоюз принял Стратегию безопасного информационного общества. Доклад 2008 года по выполнению Европейской стратегии безопасности называет кибербезопасность одним из глобальных вызовов и ключевой угрозой.[21] В марте 2010 года Совет Европы принял Европейскую Стратегию внутренней безопасности, в которой киберпреступления называются глобальной, технической, международной, анонимной угрозой для ИТ-систем. Позднее в этом же году Еврокомиссия приняла Коммюнике по Стратегии внутренней безопасности, где содержатся предложения по конкретным действиям.

В конечном итоге, защита киберпространства и цифровых инфраструктур – общая ответственность правительств, представителей частного сектора, а также региональных и международных организаций. Хотя возможны возражения, что ответственность должно взять на себя правительство, достижение успеха в этой области потребует совместных действий, включая партнерства правительств; представителей частного сектора; правительств и частного сектора, и всех их – с региональными и международными организациями. Чтобы достичь этого, необходимо создать центр обмена информацией по киберпространству, киберугрозам и уязвимым местам. Этот центр, если его создать как некоммер-

---

[20] Council of Europe, *Convention on Cybercrime*, European Treaty Series No. 185 (Budapest, 23 November 2001), режим доступа: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[21] A Strategy for a Secure Information Society –"Dialogue, partnership and empowerment," Brussels, 31 May 2006, COM(2006) 251, и Report on the Implementation of the European Security Strategy – Providing Security in a Changing World, Brussels, 11 December 2008, S407/08.

Будущий договор по киберпространству [22]

Генеральный секретарь Международного союза электросвязи (МСЭ) Хамадун Туре призвал разработать полноценный «кибердоговор», который будет содержать в себе правовые и регуляторные рамки, а также международные планы действий в чрезвычайных ситуациях на случай масштабных кибератак.

«Нам необходимы международные нормы, чтобы сделать киберпространство безопасным», – сказал Туре на недавней конференции, добавив, что ни одна нация не защищена от потенциальных угроз. «Люди, которые думают, что они в безопасности, не хотят, чтобы кто-либо говорил об этом. Но не существует он-лайн суперсилы».

Главная цель, по словам Туре, создать такой договор по киберпространству, где будет четко определено приемлемое и неприемлемое поведение и названы обязательства каждой страны по охране ее киберпространства. Туре считает, что в киберпространстве произошли серьезные изменения, а мир в настоящее время не обладает достаточными средствами, чтобы справиться с этой проблемой дипломатическими средствами.

ческое учреждение, может действовать как заслуживающий доверия координатор и посредник между всеми участниками.

Даже если удастся справиться со всеми сложными проблемами, перечисленными в этой работе, понятно, что это будет лишь верхушкой айсберга. Новые вызовы, последствия которых мы себе даже не представляем, продолжают возникать.

Как определить сущность кибератаки и обозначить реальные, эффективные и приемлемые контрмеры? В ситуации, когда очень сложно определить кто на тебя нападает, нападающий может прятаться за нейтральным посредником; когда у нападающего часто нет собственности, по которой можно нанести ответный удар – возмездия, каким мы его знали ранее, больше не существует. Значит ли это, что военные и оборонные управления должны быть на шаг впереди нападающих в условиях, когда программное обеспечение и аппаратное оборудование постоянно развиваются и обновляются? Реально ли это? Принимая во внимание время и бюджетные расходы, необходимые для разработки требуемого правительству ПО, могут ли правительства и/или военные надеяться быть более гибкими и быстрыми, чем киберпротивники? Перекладывает ли правительство свою ответственность за безопасность граждан и бизнеса на частные фирмы по кибербезопасности? Как можно остановить этот процесс?

В свою очередь, что будут означать все отмеченные действия для ИТ-сектора в целом, учитывая его стратегическую важность в экономической и военной конкуренции? Станет ли он основой новой оборонной промышленности?

Еще одна группа проблем свидетельствует о том, что киберпространство больше не является свободной, многопользовательской, межоперационной всемирной паутиной. Наметилась явная тенденция к разделению киберпро-

[22] Tim Gray, *TechNewsDaily*, 9 October 2010.

странства по различным критериям – от национальных границ и цензуры до языка и растущей популярности приложений, разработанных только для определенных устройств, что создает полузакрытые или закрытые группы пользователей Сети. Влияние этого тренда на политику кибербезопасности еще неизвестно или не исследовано. Движемся ли мы к эре интернет-протекционизма? Что это означает?

И наконец, как быть с тайной частной жизни и установлением личности в эру повышенной киберопасности? Кибероборона признается департаментами обороны и военными как следующий театр военных действий и ключевой приоритет для национальной безопасности. Как этот акцент на обеспечении кибербезопасности повлияет на существующую сегодня сеть? Новое ПО, созданное для поиска, анализа и объединения информации с социальных сетей, все чаще используется для борьбы с терроризмом, мониторинга критических ситуаций и криминальных сетей и поддержания порядка на местном, национальном и международном уровнях. Эффективность такого ПО получает все большее признание, особенно за его возможности определять поведение, предсказывать криминальную активность и выявлять террористов или преступников. Все это хорошо, но достаточно ли мы подумали о других возможностях применения новых технологий, разработанных для целей обороны. Будут ли его использовать работодатели, маркетинговые агентства и другие институции, чтобы отслеживать поведение людей на работе и в сети? Будет ли и дальше существовать частная жизнь?

3. Выводы

На основе раскрытых в данной работе проблем предлагаются некоторые основные меры, которые могут быть предприняты для усиления индивидуальной, корпоративной, национальной, региональной и международной кибербезопасности.

Меры, предлагаемые для раскрытия и мониторинга киберугроз и рисков

- Установление в режиме реального времени наблюдения, мониторинга и систем раннего предупреждения об атаках, а также инструментов для обмена важной информацией о реагировании на инциденты.
- Создание систем обнаружения вмешательств с использованием пассивных сенсоров для идентификации попыток незарегистрированных пользователей проникнуть в сети и информационные системы.
- Разработка стратегии установления подлинности личности, подтверждение паролей и права доступа для обеспечения большей уверенности в том, что только авторизованные сотрудники и органы могут получить доступ к ИТ-системам правительства и важнейших объектов инфраструктуры.
- Разработка методов поиска вредоносных кодов для долгосрочного превентивного поиска и анализа, которые не просто обнаруживают подпись, а могут определить модификации вредоносных кодов с высокой точностью и низким уровнем ложно-позитивных заключений.

Основные организации и программы, занимающиеся управлением киберпространства и безопасностью [23]

Существует около двадцати двух ключевых организаций и программ, международная деятельность которых оказывает существенное влияние на управление киберпространством и безопасность. Это далеко не все международные организации и программы по вопросам киберпространства, а лишь те, которые считаются ключевыми. К ним относят форумы по обмену информацией, которые, по сути, являются сообществами экспертов, где не принимаются решения; частные организации и созданные в результате договоренностей между странами органы, которые имеют право принимать решения. Их усилия направлены на решение проблем реагирования на инциденты, разработку технических стандартов, международное или региональное сотрудничество правоохранительных органов. Текущие программы этих организаций предполагают участие правительства и частного сектора в решении ряда проблем, таких как реализация механизмов реагирования на инциденты, разработка технических стандартов, ускорение уголовных расследований и выработка международной политики в области информационной безопасности и защиты важной инфраструктуры.

К этим основным организациям относятся:

- ✓ Азиатско-Тихоокеанское экономическое сотрудничество
- ✓ Ассоциация стран Юго-Восточной Азии
- ✓ Совет Европы
- ✓ Европейский Союз
- ✓ Европол
- ✓ Форум реагирования на инциденты безопасности
- ✓ Группа восьми
- ✓ Институт инженеров электротехники и электроники
- ✓ Международная электротехническая комиссия
- ✓ Международная организация по стандартизации
- ✓ Международный союз электросвязи
- ✓ Международная организация по доменным именам, протоколам и адресам ICANN
- ✓ Инженерный совет Интернета
- ✓ Форум по управлению Интернетом
- ✓ Интерпол
- ✓ Меридиан
- ✓ НАТО
- ✓ Организация Американских государств
- ✓ Организация экономического сотрудничества и развития
- ✓ ООН.

[23] См. приложение 1, основные направления их деятельности.

- Разработка методов определения источника вредоносных кодов либо поведения путем анализа топологии сетей и/или трафика, которые работают в условиях IP-спуфинга, большого числа «взломанных» машин, модифицированных вирусов и так далее.
- Разработка методов он-лайн обучения для динамичного моделирования, для моделирования данных при несимметричном распределении и отбора свойств данных с меняющимися характеристиками.
- Установка сканеров углубленной проверки пакетов у всех интернет-провайдеров первого уровня, которые напрямую соединены с другими интернет-провайдерами, чтобы остановить проникновения вредоносного ПО в магистраль до того, как оно попадет в сеть, которую должно атаковать.

Меры, предлагаемые для противодействия киберугрозам и рискам:

- Создание в будущем более надежной, жизнеспособной и заслуживающей доверия цифровой инфраструктуры.
- Разработка комплексных и эффективных мер и методов, которые обеспечат быстрое и неоспоримое определение источника атак.
- Разработка Стратегии кибербезопасности, задачей которой будет формирование международного климата и объединение позиций стран-союзниц по вопросам технических стандартов, приемлемых норм, суверенных обязательств и применения силы.
- Проведение комплексных проверок по выявлению слабых мест ключевых ресурсов и важной инфраструктуры, включая оценку рисков для определения степени риска атак определенного типа.
- Разработка комплексного национального плана ликвидации этих слабых мест.
- Установление приоритетности защиты, признание того, что не все объекты важны в равной степени, а расходы на защиту объектов должны быть соизмеримы с выгодами от усиления защиты от угрозы.
- Объединение всей соответствующей информации, анализа и оценок уязвимости с целью определить приоритетные меры защиты и поддержки, способы уменьшения потенциальных рисков, их значимость с точки зрения экономической эффективности.
- Лучшее определение ролей, ответственности правительства в обеспечении безопасности объектов важной инфраструктуры, правительственных сетей и ИТ- систем.
- Обеспечение безопасности сетей и ИТ-систем путем уменьшения числа потенциальных и реальных слабых мест, защиты от попыток проникновения, предсказывания будущих угроз; выяснение тенденций путем содействия исследованиям и развитию, образованию и инвестициям в революционные технологии.
- Исправление недостатков в оценке рисков, в политике и процедурах защиты информационных технологий, планировании безопасности, тре-

нингах по безопасности, тестировании и оценке систем, восстановительных действиях и руководствах.

- Решение проблем ИТ-безопасности, связанных с идентификацией и подтверждением личности пользователя, авторизацией, защитой границ памяти, аудитом и мониторингом, криптографией, физической безопасностью, разделением обязанностей, управлением конфигурацией системы и планом действий в чрезвычайных ситуациях.
- Защита от нарушения нормального функционирования ИТ-систем объектов важной инфраструктуры, а также обеспечение того, что такие нарушения будут происходить не часто, будут недлительными, управляемыми и приведут к минимальным потерям.
- Проведение целенаправленных и совместных исследований и разработок в области обеспечения безопасности объектов важнейшей инфраструктуры должно стать национальным приоритетом, при этом необходимо помнить о краткосрочных, промежуточных и долгосрочных приоритетах, привлечении академической науки и частного сектора и соответствии Стратегии кибербезопасности.
- Создание рабочих групп по проведению ежегодных обзоров исследовательских инициатив в секторах и подготовке рекомендаций по обновлению приоритетов на основе изменений в технологиях, угрозах, рисках и выявленных слабых местах.
- Привлечение частного сектора к проведению периодических оценок слабых мест важных систем ИТ и телекоммуникаций их сегмента ВНИ.
- Определение системы показателей и способов выявления эффективности проектов обеспечения безопасности сетей и ИТ-систем; отслеживания прогресса, что позволит создать стимулы для изменения поведения организаций и отдельных лиц и своевременного представления отчетов о результатах исследований.
- Проведение проверок работы в соответствии с общепринятыми стандартами правительственного мониторинга.
- Создание эффективной системы координации и обмена информацией между общественными институтами и частным сектором в ответ на серьезные киберинциденты.

Меры, необходимые для решения юридических проблем:

- Создание, пересмотр и модернизация уголовного законодательства; процедур проведения электронных расследований; политики обеспечения функциональности мер предотвращения, сдерживания, реагирования и преследования в судебном порядке киберпреступлений как на национальном, так и на международном уровнях.
- Создание приемлемых правовых норм расследования киберпреступлений с точки зрения территориальной юрисдикции, суверенных обязательств и применения силы.

- Создание специализированных подразделений по борьбе с киберпреступлениями, подготовка групп электронных криминалистов, проведение тренингов и налаживание связей со всеми, кто имеет отношение к организации единого реагирования на киберпроисшествия и сдерживанию киберпреступлений, включая юстицию и частный сектор.
- В сотрудничестве с правительственными экспертами и экспертами гражданского общества по вопросам защиты личной информации создание, пересмотр и модернизация правовых инфраструктур, связанных с защитой информации, личных данных, цифровых подписей, торговым правом, электронным государством и шифрованием.
- Гармонизация различных национальных законов о расследовании и преследовании в судебном порядке киберпреступлений, защите информации, сохранении личных данных; нахождение компромисса с принятыми в других странах законами, которые не предусматривают наказания за киберпреступления.
- Разработка механизмов сотрудничества между агентствами в сфере участия и обмена информацией в ходе расследований киберпроисшествий.
- Разработка скоординированного всеправительственного подхода к взаимодействию с международными организациями в сфере обеспечения кибербезопасности, что предусматривает усиление сотрудничества правоохранительных органов и профессионалов в области кибербезопасности из разных стран, создание стандартов безопасности и выполнение международных соглашений по участию и обмену информацией.
- Разработка процедур согласования и улучшения правил участия, обсуждения соответствующих проектов с правительствами других стран и координации реагирования на международные киберинциденты.
- Помощь в разработке международных норм и стандартов, содействие международному и региональному сотрудничеству.
- Упорядочивание и уточнение тех элементов правовой структуры, которые способствуют проведению расследований, включая снятие юридических барьеров для выявления источника атаки и электронного преследования хакеров.

Меры, необходимые для привлечения квалифицированных сотрудников и акцентуации внимания общественности на проблеме кибербезопасности:

- Решение основных проблем в привлечении, найме, подготовке, переподготовке и эффективном управлении работой талантов в области кибербезопасности и криминалистики, создание для них привлекательных карьерных перспектив.
- Достижение согласия всех сторон о масштабе усилий в области образовательных проектов, цель которых – обеспечить подготовку сотрудников, умеющих защищать ИТ-системы; формирование приоритетов и перенаправление образовательных усилий для подготовки квалифицированного персонала и осуществление дальнейшей подготовки талантливых ученых в государственных интересах.

- Начало национальной образовательной кампании по привлечению внимания к проблеме кибербезопасности, усиление поддержки образовательных программ, а также исследований и разработок, которые обеспечат конкурентоспособность страны в информационную эру.

Ключевые этапы разработки Стратегии кибербезопасности:

- Разработать Стратегию кибербезопасности, в которой четко названы стратегические цели, задачи и приоритеты.
- Установить ответственность правительства на высшем уровне за руководство и контроль над национальной политикой кибербезопасности.
- Создать правительственные структуры, занимающиеся вопросами реализации Стратегии кибербезопасности.
- Привлекать внимание к серьезности проблемы кибербезопасности.
- Создать действенную организацию, которая отвечает за реализацию кибербезопасности.
- Сконцентрировать внимание на определении приоритетности объектов, оценке уязвимых мест и снижении их числа, а не на разработке дополнительных планов.
- Содействовать сотрудничеству общественных институтов и частного сектора путем повышения ценности предложений и применения большего количества стимулов.
- Уделять больше внимания решению глобальных проблем кибербезопасности.
- Повысить эффективность работы правоохранительных органов по борьбе со злонамеренными действиями в киберпространстве.
- Больше внимания уделять исследованиям и разработкам в области кибербезопасности, включая изучение проблемы улучшения координации усилий правительства и частного сектора.
- Увеличить число профессионалов в области кибербезопасности и криминалистики.
- Правительство должно стать моделью обеспечения кибербезопасности и безопасности ВНИ, особенно при совершении закупок необходимо оценивать приобретаемые продукты и услуги с точки зрения кибербезопасности.

Приложение

ОСНОВНЫЕ ОРГАНИЗАЦИИ И ПРОГРАММЫ, КОТОРЫЕ ОКАЗЫВАЮТ БОЛЬШОЕ ВЛИЯНИЕ НА УПРАВЛЕНИЕ КИБЕРПРОСТРАНСТВОМ И КИБЕРБЕЗОПАСНОСТЬЮ

Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС)

АТЭС – экономический и торговый форум, задачей которого является содействие экономическому росту и сотрудничеству 21 страны Азиатско-Тихоокеанского региона. Рабочая группа по телекоммуникациям и информации (ТЕЛ) АТЭС занимается координацией действий по обеспечению безопасности информационной инфраструктуры стран-участниц путем поддержки действий, направленных на развитие потенциала эффективного реагирования на инциденты, разработку стандартов информационной безопасности, борьбу с киберпреступлениями, мониторинг потенциальных проблем, возникающих с развитием технологий, усиление международного сотрудничества в сфере обеспечении кибербезопасности. Некоторые из этих программ ТЕЛ осуществляет совместно с другими международными организациями, такими как АСЕАН, МСЭ и ОЭСР.

Ассоциация стран Юго-Восточной Азии (АСЕАН)

АСЕАН – экономическая организация 10 стран Юго-Восточной Азии, которая также занимается вопросами безопасности. В соответствии с планом действий АСЕАН на 2009-2015 годы, ее задачей является борьба с транснациональной киберпреступностью на основе сотрудничества правоохранительных органов стран-участниц и совместных усилий по принятию законодательства в сфере киберпреступности. Кроме того, план действий предусматривает деятельность по развитию информационных инфраструктур и увеличение в странах АСЕАН числа компьютерных групп реагирования на чрезвычайные ситуации (CERT), а также проведение соответствующих тренингов.

Совет Европы

Совет Европы – организация, в состав которой входит 47 стран, создана в 1949 году для разработки общих демократических принципов защиты личности. В 2001 году Советом Европы была принята Конвенция по киберпреступлениям с целью улучшения международного сотрудничества по борьбе с действиями, направленными против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных. В Конвенции дано согласованное определение преступлений в киберпространстве, которые должны считаться наказуемыми согласно внутреннему законодательству стран. К таким действиям относятся несанкционированный доступ к компьютерным системам, мошенничество, совершенное в киберпространстве, действия, связанные с детской порнографией и нарушением авторских прав. Совет Европы также выступает спонсором тренингов и конференций по вопросам кибербезопасности.

Полицейская служба Европейского Союза (Европол)

Европол, Полицейская служба Европейского Союза (год создания – 1992), – специализированный институт Евросоюза, задачей и целью которого является содействие международному сотрудничеству полиции в борьбе с организованной преступностью, терроризмом и киберпреступностью. Миссия Европола – внести значительный вклад в разоблачение, предупреждение и привлечение к суду организованной преступности; борьба с организованными преступными организациями. Европол оказывает помощь государствам-участникам при помощи обмена разведывательной информацией с офицерами связи Европола, откомандированными в штаб-квартиру в Гааге государствами-участниками в качестве представителей их национальных правоохранительных агентств. В июне 2010 года было создано Европейское спецподразделение по борьбе с киберпреступностью, в составе которого действует Система он-лайн информирования об интернет-преступлениях (ICROS), аналитическая картотека киберпреступности (Analysis Work File Cyborg), которая активно используется в борьбе с преступными группами, действующими в Интернете, и Форум интернет-экспертов и экспертов-криминалистов (IFOREX) для размещения технических данных и проведения тренингов для правоохранителей, занимающихся вопросами киберпреступности. Стратегия Европола на 2010-2014 годы предусматривает план усиления потенциала борьбы с киберпреступностью, создание в рамках Европола Европейского Центра по борьбе с киберпреступностью, задача которого – обеспечение координации и эффективности усилий по борьбе с киберпреступностью на европейском уровне. Этот центр будет использовать новые средства обработки информации и создаст базу данных по интернет-сайтам, представляющим киберугрозу. Европол обеспечивает оперативный анализ, обмен опытом и техническую поддержку расследований и операций в пределах Евросоюза; готовит доклады по стратегиям и аналитические обзоры преступлений на основе информации и материалов разведки, предоставленных такими национальными правоохранительными органами, как полиция, таможня, иммиграционные службы, либо полученных из других источников. Чтобы эффективно противостоять международной организованной преступности, Европол сотрудничает с некоторыми третьими странами и институтами, такими как Европейский центральный банк, Европейский мониторинговый центр по наркотикам и наркомании, Европейское бюро по борьбе с мошенничеством (OLAF), Управление ООН по наркотикам и преступности, Объединенный ситуационный центр Евросоюза, Всемирная таможенная организация и мн. др.

Европейский Союз

Евросоюз – экономическое и политическое объединение 27 европейских стран. Подкомитеты его исполнительного органа – Европейской комиссии – должны заниматься вопросами кибербезопасности, чтобы улучшить 1) готовность и предотвращение, 2) выявление и ответ, 3) минимизацию последствий и восстановление, 4) международное сотрудничество, 5) критерии важных объектов Европейской инфраструктуры в секторе информационно-коммуникационных технологий. Еврокомиссия определит приоритеты международного участия, включая взаимопомощь, усилия по восстановлению и управление в кризисной ситуации. Она также создала Европейское агентство по сети и информационной безопасности (ENISA), независимое Европейское агентство, цель которого – усиление потенциала его участников в решении проблем безопасности сетей и информа-

ции. Созданное в 2004 году, ENISA должно на международном уровне заниматься вопросами защиты и устойчивости информационных инфраструктур, привлечением внимания к проблеме и обеспечением обмена информацией между участниками. Более того, в Евросоюзе существует несколько независимых организаций, которые занимаются разработкой технических стандартов. Европейский комитет по стандартизации ведет работу по снятию торговых барьеров для промышленности Европы и созданию платформы для разработки Европейских стандартов и технических спецификаций. Европейский комитет по стандартизации в электротехнической и электронной промышленности – некоммерческая техническая организация, занимающаяся подготовкой рекомендательных стандартов на электрические и электронные товары и услуги на европейском рынке. Европейский институт телекоммуникационных стандартов – некоммерческая организация, в задачи которой входит разработка мировых стандартов для информационных и коммуникационных технологий, включая Интернет.

Форум реагирования на инциденты безопасности (FIRST)

Форум является международным объединением отдельных групп реагирования на инциденты безопасности, которые обмениваются технической информацией и информацией о проблемах безопасности. В нем участвуют 220 представителей из 42 стран. Участники представляют правительства, правоохранительные органы, науку, частный сектор и другие организации. Руководящий комитет Форума отвечает за общую политику работы, процедуры и другие вопросы, регулирующие деятельность организации. FIRST сотрудничает со многими стандартизационными организациями в сфере разработки стандартов кибербезопасности, управления инцидентами и реагирования. Кроме того, он использует Систему ранжирования рисков в качестве стандарта определения ИТ-рисков, что помогает при обмене информацией о рисках и их характеристиках.

Группа восьми (G8)

G8 – международный форум, в работе которого принимают участие правительства Канады, Франции, Германии, Италии, Японии, России, Великобритании и США. Работа G8 по обеспечению кибербезопасности осуществляется под руководством Группы по высокотехнологическим преступлениям, задачей которой является предупреждение, расследование и привлечение к ответственности тех, кто совершает преступления при помощи компьютеров, сетевых сообществ и других новых технологий. В 1997 году группа организовала 24/7 Сетевой контактный центр высокотехнологичных преступлений, который позволяет представителям правоохранительных органов – не только стран участниц G8 – быстро связаться со своими коллегами для получения/оказания помощи в расследовании киберпреступлений. Сетевой контактный центр является вспомогательным инструментом предоставления/получения помощи от правоохранительных органов. В 2004 году группа также разработала руководство по сетевой безопасности, чтобы помочь операторам сетей и системным администраторам адекватно реагировать на компьютерные инциденты. А в 2006 году во время своего председательства в G8 Россия выдвинула инициативу сотрудничества общественных институтов и частного сектора в борьбе с терроризмом и организованной преступностью; обеспечение кибербезопасности было признано одним из трех приоритетов наряду с защитой систем энергоснабжения и кибераспектами безопасности движения через границы людей, товаров и денег.

Институт инженеров электротехники и электроники (IEEE)

Институт является профессиональной ассоциацией, занимающейся электротехническими и компьютерными науками, инженерией и смежными науками. К его деятельности, связанной с кибербезопасностью, относится разработка технических стандартов через Ассоциацию стандартов ИИЭЭ, базирующейся в своей деятельности на принципе консенсуса. Среди прочих разработаны всемирно признанные стандарты беспроводных сетей и шифрования. Ассоциация стандартов ИИЭЭ совместно с Национальным институтом стандартов и технологий (США) принимала участие в разработке стандартов кибербезопасности для систем контроля электроэнергетических компаний.

Международная электротехническая комиссия (IEC)

МЭК готовит и публикует международные стандарты для электротехники, электронных и смежных технологий. Ее членами являются национальные комитеты более 70 стран, в состав которых входят представители частного и государственного сектора каждой страны. МЭК и Международная организация по стандартизации (ISO) через Совместный технический комитет (JTC) разработали стандарты информационной безопасности для всех типов организаций, включая коммерческие предприятия, правительственные агентства и некоммерческие организации. Например, один из таких совместно разработанных стандартов касается создания, обслуживания систем управления информационной безопасностью и соблюдения режима секретности. Этот стандарт может быть применен во всех организациях, независимо от их размера.

Международная организация по стандартизации (ISO)

МОС – неправительственная организация, занимающаяся разработкой и изданием международных стандартов. В процессе принимают участие национальные институты стандартизации 162 стран, руководит работой Генеральный секретариат, расположенный в Женеве, решения принимаются методом консенсуса. Стандарты ISO применяются в традиционных сферах, таких как сельское хозяйство и строительство, а также в области информационных и коммуникационных технологий.

Международный союз электросвязи (ITU)

МСЭ – агентство ООН, задачей которого является разработка технических стандартов, распределение радиочастот, а также развитие технического потенциала и оказание помощи развивающимся странам. Три сектора выполняют эти миссии, разрабатывая рекомендации: Сектор телекоммуникационной стандартизации МСЭ (ITU-T), Сектор радиокоммуникации МСЭ (ITU-R) и Сектор развития телекоммуникаций МСЭ (ITU-D). Кроме этого, Генеральный секретариат МСЭ осуществляет руководство на высшем уровне, чтобы обеспечить гармонизацию институционных стратегий во всех секторах. Членами МСЭ являются делегации 191 страны, а также 700 представителей частного сектора. МСЭ были разработаны технические стандарты безопасности; также оказывалось содействие в других сферах обеспечения кибербезопасности. Например, в Секторе телекоммуникационной стандартизации создана исследовательская группа по изучению безопасности телекоммуникаций, которая занимается разработкой стандартов и рекомендаций, связанных с безопасностью информаций и сетей, применением мер безопасности и управлением учетными записями. Сектор развития теле-

коммуникаций подготовил доклад о лучших методах обеспечения кибербезопасности для стран, пытающихся создать подобные системы. А Генеральный секретариат МСЭ опубликовал Глобальную программу кибербезопасности (GCA), которая должна помочь в создании единого скоординированного международного подхода к кибербезопасности во всех секторах МСЭ. Программа затрагивает пять аспектов: 1) законодательные меры, 2) технические и процедурные мероприятия, 3) организационные структуры, 4) создание потенциала и 5) международное сотрудничество. Более того, Генеральный секретариат подписал Меморандум о взаимопонимании с Международным многосторонним партнерством против киберугроз (ИМПАКТ), согласно которому будет создан оперативный центр по координации реагирования на инциденты и предоставлению странам-участницам и представителям частного сектора информации о киберугрозах.

Международная организация по доменным именам, протоколам и адресам (ICANN)

ICANN (США) – частная некоммерческая корпорация, основной задачей которой является координирование технического руководства доменными именами и системой адресации. Ее работой руководит Совет директоров, в состав которого входит 21 представитель, 15 из них имеют право голоса, а 6 являются координаторами без права голоса. ICANN в 2009 году подписал с Департаментом торговли США Соглашение об обязательствах, которое завершило передачу технического руководства Системой доменных имен (DNS) в руки частного сектора. Управление будет осуществляться с многосторонним участием, что должно гарантировать ответственность и прозрачность процесса принятия решений, направленных на защиту интересов интернет-пользователей всего мира. ICANN оказывает содействие в разработке политики Системы доменных имен в ходе восходящего процесса, учитывающего интересы регистраторов доменов верхнего уровня, регистраторов доменных имен, региональных интернет-регистраторов, технического сообщества, бизнес- и частных пользователей Интернета, правительств. ICANN также по соглашению с Департаментом торговли США выполняет функции полномочного органа по присвоенным именам. Кроме того, корпорация выполняет нескольких независимых функций управления Интернетом, включая координирование присвоения параметров технических протоколов, управление корневыми доменами и распределение интернет-ресурсов.

Инженерный совет Интернета (IETF)

Инженерный совет Интернета – орган по созданию технических стандартов – отвечает за разработку и соблюдение основных стандартов Интернета, включая протоколы системы доменных имен и их спецификации, обеспечивающие безопасность, а также нынешнюю и последующие версии интернет-протокола. Основные стандарты, которые разрабатывает IETF, определяют на базовом уровне как функционирует Интернет, какие функции он может выполнять. IETF является добровольным органом, его стандарты приняты по методу консенсуса, а в работе участвуют операторы сетей, ученые и представители правительства и отрасли. Большая часть работы IETF осуществляется при помощи электронных рассылок, хотя каждый год в различных странах проводятся три встречи его членов.

Форум по управлению Интернетом (IGF)

В программе, принятой на Мировом саммите информационного общества (Тунис, 2005 год), предусмотрено создание Генеральным секретарем ООН Форума по управлению Интернетом многосторонней площадки для обсуждения ключевых вопросов управления Интернетом. Широкое участие в IGF и акцент на обмен информацией позволяют этой структуре играть роль форума исключительной важности, где правительства, частный сектор, организации гражданского общества и частные лица принимают участие в открытых обсуждениях, в задачи которых не входит достижение конкретного политического результата. И хотя результатом ежегодных встреч не являются стандарты, рекомендации либо обязательные к исполнению соглашения, идеи, выработанные IGF, могут быть в дальнейшем применены другими международными организациями.

Интерпол

Интерпол – крупнейшая мировая организация полиции, созданная для облегчения международного сотрудничества. Он собирает, обобщает, анализирует и организовывает обмен информацией по киберпреступлениям между 188 своими участниками, использующими глобальную коммуникационную систему полиции. Интерпол также отвечает за координацию оперативных ресурсов, таких как компьютерный криминалистический анализ при расследовании киберпреступлений. С Интерполом сотрудничают следователи национальных подразделений по расследованию преступлений, совершенных с использованием компьютеров; Интерпол оказывает помощь в максимально быстром получении цифровых доказательств и проведении расследований кибератак, происходящих в смешанных юрисдикциях. Для разработки стратегий противодействия киберпреступлений, совершенных на основе новейших методов, группы экспертов объединяются в региональные рабочие группы, чтобы использовать региональный опыт коллег из Европы, Азии, обеих Америк, Ближнего Востока и Северной Африки. Рабочие группы обмениваются информацией о региональных трендах киберпреступности, налаживают сотрудничество между странами-участницами и разрабатывают учебные материалы для правоохранительных органов.

Меридиан

Процесс и Конференция «Меридиан» возникли в 2005 году для обмена идеями и разработки планов межправительственного сотрудничества в сфере обеспечения защиты важнейшей информационной инфраструктуры мира. Ежегодная конференция и промежуточные мероприятия проводятся каждый год, чтобы построить доверие и наладить отношения между участниками, а также способствовать обмену опытом по защите мировой важнейшей информационной инфраструктуры. Участие в Процессе «Меридиан» открыто для всех стран и предполагает уровень участия высших политиков. Конференция позволяет воспользоваться преимуществами и возможностями сотрудничества между правительствами и обменяться опытом. Задачей Процесса «Меридиан» также является объединение усилий в работе над специфическими темами, такими как *безопасность систем контроля*.

НАТО

НАТО – Альянс 28 стран Северной Америки и Европы. В 2008 году была одобрена политика кибероборонны, в которой изложены рекомендации для членов Аль-

янса по защите ключевых информационных систем по противодействию кибератакам. Особо оговорено создание органа по управлению кибербезопасностью, который обладает полномочиями для управления кризисами в кибероборонe, включая Центр НАТО по реагированию на компьютерные инциденты. После того как правительственная, правоохранительная, банковская, медиа- и интернет-инфраструктуры Эстонии в течение трех недель апреля страдали от кибератак, НАТО призвало к созданию государственных органов по кибероборонe для обмена информацией, формирования возможностей взаимопомощи в случае киберинцидента, определения коммуникационных и информационных систем, которые будут управлять особо важной для Альянса информацией.

Организация Американских государств (OAS)

Организация американских государств – неправительственная организация, в состав которой входят 34 страны Северной, Центральной и Южной Америки, а также островов Карибского бассейна. В 2004 году участники ОАГ приняли Всеобъемлющую межамериканскую стратегию кибербезопасности, в которой кибербезопасность названа проблемой, имеющей все большую важность для членов ОАГ и предполагающей участие в ее исследовании 3 органов ОАГ. Стратегия предусматривает, что Межамериканский комитет по борьбе с терроризмом разработает план создания Команд реагирования на инциденты безопасности, которые будут действовать во всем полушарии 24 часа в сутки 7 дней в неделю. Кроме этого, Межамериканская комиссия по телекоммуникациям должна оценить существующие технические стандарты кибербезопасности, рекомендовать к принятию особенно важные из них и определить, что препятствует применению этих стандартов в обеих Америках. И последнее, Стратегия предусматривает, что встреча министров юстиции, других министров или генеральных прокуроров Американских государств, при посредничестве Группы правительственных экспертов по кибербезопасности должна обеспечить техническую помощь государствам-участникам в разработке и применении эффективных законов по киберпреступности для защиты информационных сетей и усовершенствования процессов расследования и привлечения к суду.

Организация экономического сотрудничества и развития (OECD)

ОЭСР – межправительственная организация, в состав которой входит 31 демократическая страна. Правительства стран-участниц имеют возможность сравнить опыт применения политик, ищут ответы на общие вопросы, определяют лучший опыт и координируют внутреннюю международную политику. Рабочая группа ОЭСР по информационной безопасности и неприкосновенности частной жизни (WPISP), применяя метод консенсуса, разрабатывает предложения по политике информационной безопасности и неприкосновенности частной жизни в условиях все большего использования информационных и коммуникационных технологий. Кроме анализа предлагаемой политики ОЭСР отвечает за разработку рекомендаций для стран-участниц по улучшению безопасности и защите неприкосновенности частной жизни. Так, например, в 2008 году Совет ОЭСР принял рекомендации, призывающие страны-участницы к сотрудничеству между собой и с представителями частного сектора для улучшения защиты объектов важнейшей инфраструктуры. В частности, рекомендации содержали призыв к двустороннему и многостороннему обмену опытом, развитию понимания взаимозависимости и слабых мест и определению национальных агентств, за-

нимающихся защитой важнейшей информационной инфраструктуры, осознанию важности систем международного наблюдения и предупреждения, а также к международному сотрудничеству в области киберисследований и разработок.

ООН

ООН – международная организация, в состав которой входит 192 страны, была основана в 1945 году. Ее задачей является поддержание международного мира и безопасности, развитие дружественных отношений между странами, содействие социальному прогрессу, повышению стандартов жизни и защита прав человека. Генеральная ассамблея, которая является форумом для обсуждения и принятия резолюций по вопросам кибербезопасности и привлечения внимания к этой проблеме, – главный совещательный, представительный и политический орган. В 2005 году Межрегиональный научно-исследовательский институт ООН по вопросам преступности и правосудия начал изучение проблем киберпреступности и разработку проекта «Создание профиля хакера» (HPP). Другие подразделения ООН, такие как Бюро по борьбе с наркотиками и преступностью, являются дополнительными форумами, где страны-участницы могут обсудить подходы к решению транснациональных проблем, включая киберпреступность.

О серии «Горизонт 2015»

В серии ДКВС «Горизонт – 2015» изучается роль различных частных и других негосударственных организаций в реагировании на новейшие вызовы безопасности. Цель проекта – расширить аналитический горизонт за пределы существующих подходов к реформированию и управлению сектором безопасности. Необходимо выйти за рамки первой революции в этой сфере, которая привела к использованию «всеправительственного» подхода, и двигаться ко второй революции, которая приведет к совместному разрешению проблем всеми институтами сектором безопасности – не только правительственными структурами, но и определенными частными компаниями, – что позволит применить так называемый «всесторонний подход к проблеме».

В рамках проекта ДКВС «Горизонт – 2015» в 2010 и 2011 годах проводились тематические круглые столы с участием соответствующих правительственных и неправительственных организаций. По результатам каждого круглого стола готовились соответствующие тематические публикации, в которых приводится краткое введение в проблему, предшествующее изучению теоретических и практических вопросов, связанных с прозрачностью контроля, ответственностью и демократическим управлением в целом. Тематические публикации, конечно же, не имеют целью решить поставленную проблему, они должны стать платформой для дальнейшей работы и исследований. Как таковые, они могут содержать больше вопросов, чем ответов. Кроме этих тематических публикаций в рамках проекта была издана работа «*Тренды и вызовы международной безопасности: перечень*» *(Trends and Challenges in International Security: An Inventory).* Работа доступна на сайте, режим доступа: www.dcaf.ch/Publications. Задача этой публикации – дать описание современных проблем безопасности и стать информационной базой проекта в целом.

Кроме этого в этой серии:

- ✓ *Democratic Challenges of Cyber Security* (Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler)
- ✓ *Public Private Cooperation: Challenges and Opportunities in Security Governance* (Benjamin S. Buckland, Theodor H. Winkler)
- ✓ *Private Military & Security Companies: Future Challenges in Security Governance* (Anne-Marie Buzatu, Benjamin S. Buckland)

Фред Шрайер, Барбара Викс, Теодор Х. Винклер, *Кибербезопасность: дорога, которую предстоит пройти* (Женева: Женевский центр демократического контроля над вооруженными силами, 2013).

DCAF Horizon 2015 Working Paper No. 4.RU

Язык оригинальной версии: английский, Женева, 2011

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 978-92-9222-235-2

Женевский центр демократического контроля над вооруженными силами (ДКВС)

ДКВС был основан в 2000 году швейцарским правительством. ДКВС – международная организация, в которую входят 61 государство и швейцарский кантон Женева. Главными подразделениями ДКВС являются отделы исследовательских, оперативных и специальных программ. Штат Центра составляют более 100 человек из 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 службы и вооруженные силы.

www.dcaf.ch

Эта публикация подготовлена благодаря финансовой поддержке Директората политики безопасности – Федерального Департамента обороны, защиты населения и спорта Швейцарии