Управление библиотечных фондов (Парламентская библиотека)

БИБЛИОДОСЬЕ

Подготовлено по запросу
Комитета Совета Федерации
по науке, образованию, культуре
и информационной политике
к «круглому столу» на тему

«О разработке стратегии национальной кибербезопасности Российской Федерации: состояние, предпосылки, механизмы и перспективы»

по информационно-библиографическим ресурсам
Управления библиотечных фондов
(Парламентской библиотеки)

Москва,
февраль 2013 г.

Предлагаемое библиодосье к «круглому столу» на тему **«О разработке стратегии национальной кибербезопасности Российской Федерации: состояние, предпосылки, механизмы и перспективы»** подготовлено по запросу Комитета Совета Федерации по науке, образованию, культуре и информационной политике на основе информационно-библиографических ресурсов Управления библиотечных фондов (Парламентской библиотеки).

Библиодосье состоит из трех частей.

Первая часть содержит публикации в журналах, газетах и интернет-ресурсах о государственной политике и направлениях разработки стратегии кибербезопасности в Российской Федерации, обеспечении кибербезопасности органов государственной власти, возможных вариантах защиты пользователей от кибератак, проблемах применения административного и информационного законодательства в сфере безопасности в киберпространстве, а также о действующих государственных стратегиях кибербезопасности зарубежных государств.

Вторая часть включает статистические и справочные материалы о состоянии интернет-безопасности в Российской Федерации, об утечках корпоративной информации и конфиденциальных данных, в том числе в банковском секторе.

В **третьей части** представлен дополнительный список книг, авторефератов диссертаций, неопубликованных материалов парламентских мероприятий, публикаций в сборниках, журналах, газетах и интернет-ресурсах по вопросам обеспечения информационной безопасности и предотвращения киберугроз. Библиографические записи расположены в алфавитном порядке авторов или заглавий.

СОДЕРЖАНИЕ*

Составители:
Научное редактирование - канд. филол. наук ***Т.А. Москаленко*** *(начальник отдела библиотечно-информационного обслуживания УБФ (ПБ);*
Поиск, анализ, отбор, систематизация материалов в ресурсах УБФ (ПБ), полнотекстовых базах данных, формирование библиографических списков, оформление библиодосье - ***А.А. Якушина*** *(ведущий специалист 3 разряда отдела библиотечно-информационного обслуживания УБФ (ПБ); подготовка статистических и справочных материалов -* ***Е.Л. Малахова*** *(консультант отдела ведения баз данных и государственной библиографии по официальным документам УБФ (ПБ);*
Сканирование публикаций, подготовка электронной версии библиодосье, размещение на сайте УБФ (ПБ) в сети Интранет Государственной Думы по адресу: http://parlib-search.duma.gov.ru/ - ***С.А. Домченков*** *(консультант отдела электронных изданий УБФ (ПБ);* ***А.В. Ильин*** *(старший специалист 2 разряда отдела библиотечно-информационного обслуживания УБФ (ПБ).*

Контакты: *тел. 8-495-692-68-75, факс. 8-495-692-97-36, e -mail: parlib@duma.gov.ru*

*В материалах, использованных для подготовки библиодосье, сохранены оригинальные тексты источников опубликования.

Часть I

Публикации в журналах, газетах и интернет-ресурсах

СОВЕТ ФЕДЕРАЦИИ ЗАНЯЛСЯ ЦИФРОВЫМ СУВЕРЕНИТЕТОМ*

О направлениях разработки стратегии кибербезопасности Российской Федерации

(извлечение)

М. Иванов

В комиссии Совета Федерации по развитию информационного общества, которая готовит стратегию кибербезопасности РФ, определились с основными угрозами, которые могут быть нанесены в сфере информационных технологий как отдельным гражданам, бизнесу, так и государству в целом. По словам главы комиссии Руслана Гаттарова, целью стратегии должен стать «цифровой суверенитет» РФ.

В предварительном плане стратегии кибербезопасности угрозы распределены по трем направлениям. Первое касается угроз гражданам: это утечка и обнародование частной информации, мошенничество, распространение опасного контента, воздействие на личность «путем сбора персональных данных» и «атаки на инфраструктуру, используемую гражданами в обычной жизни». Среди опасностей для российского бизнеса названо «воздействие на системы интернет-банкинга», блокирование систем покупки билетов, онлайн-торговли, геоинформационных систем и хакерские атаки на частные сайты.

В качестве типичной угрозы для граждан глава профильной комиссии Совета Федерации (СФ) Руслан Гаттаров приводит зарубежные интернет-сервисы: «В соглашении с Gmail пользователь официально разрешает читать его почту, чтобы компания могла подбирать под него контекстную рекламу. Гипотетически все, что есть у пользователя на почте, может быть использовано в интересах третьих лиц». Это, по мнению сенатора, может быть использовано и для шантажа, и для коммерческого шпионажа. «А если, например, упадет «Яндекс», где у людей почта, карты, афиши, то они будут винить не только компанию и хакеров, но и власть»,- пояснил «Ъ» господин Гаттаров.

В плане стратегии выделено и пять основных угроз, которые могут нанести вред всему государству. Это «атаки на ключевые государственные системы управления - электронное правительство, сайты госорганов», «экономическая блокада - масштабное отключение платежных систем, систем бронирования», «аппаратная атака на персональные компьютеры, смартфоны граждан и организаций», атаки на бытовые объекты, которые управляются с помощью информационно-коммуникационных технологий, и «критически важную инфраструктуру».

Инфраструктура безопасности, согласно плану, должна включать аппаратную и программную «платформы». Это не значит, что все «железо» и все программное обеспечение должно обязательно производиться в России, но оно «должно передаваться нам со всеми исходными кодами», чтобы было понятно, как и зачем оно может быть использовано, пояснил Руслан Гаттаров. Эту проблему в 2011 году поднимали представители ФСБ. В частности, они заявляли о том, что использование зарубежных интернет-сервисов вроде Gmail и Skype угрожает национальной безопасности: правоохранители не могут оперативно расшифровывать сообщения таких сервисов, а это активно используется участниками экстремистских и других организаций (см. «Ъ» от 9 апреля 2011 года). Также, согласно плану, в инфраструктуру кибербезопасности РФ будут входить «корневая инфраструктура интернета» и «медиаструктура интернета». «То есть должна быть создана такая инфраструктура, чтобы система не зависела от одного кабеля, а в случае ЧП могла перераспределить нагрузку для бесперебойной работы российского интернета»,- объяснил господин Гаттаров. То есть стратегия должна гарантировать «цифровой суверенитет».

---

*Иванов М. Совет Федерации занялся цифровым суверенитетом: извлечение / М. Иванов // Коммерсант. Daily. - 2012. - 6 нояб. - С. 3

Предварительный план стратегии уже разослан представителям госорганов и IT-рынка. «Когда рабочая группа наполнит ее своими предложениями, проект появится для обсуждения на специальном интернет-ресурсе»,- сообщил сенатор. В итоге в стратегии будут подробно прописаны все угрозы, варианты их локализации, рекомендации бизнесу, гражданам и госструктурам, что делать в том или ином случае.

«Апгрейд стратегии информационной безопасности, конечно, нужен, и замечательно, что в СФ этой работой занимаются»,- заявили «Ъ» в Минсвязи. При этом собеседник «Ъ» отметил, что в правительстве над безопасностью в сфере информационных технологий (IT) идет своя, закрытая работа. Заместитель секретаря генсовета «Единой России», член думского комитета по информационной политике Сергей Железняк пояснил «Ъ», что работа по вопросам IT-безопасности ведется на нескольких площадках и предложения от них «будут формировать наиболее прагматичный вариант решения существующих проблем».

Гендиректор Infowatch Наталья Касперская заявила «Ъ», что доктрина информационной безопасности, подписанная президентом Путиным еще в 2000 году, нуждается в адаптации, «ведь появились новые угрозы». (…)

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В РФ: СЛОЖНОСТИ И ПЕРСПЕКТИВЫ*

А. Колесников, директор Координационного центра национального домена сети Интернет

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

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

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

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

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

*Колесников А. Информационные технологии в РФ: сложности и перспективы / А. Колесников // Индекс безопасности. - 2013. - № 1. - С. 17-22 (из фондов Научной электронной библиотеки *http://elibrary.ru*)

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

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

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

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

Мы изучили опыт 11 ведущих *кибердержав* и пришли к неутешительному выводу: Российская Федерация серьезно отстала в области разработки и внедрения единых методов и стандартов обеспечения кибербезопасности. В Стратегии национальной безопасности Российской Федерации до 2020 г. и упомянутой Доктрине повестке кибербезопасности практически не нашлось места. В частности, не урегулированы и нормативно не закреплены проблемы оперативной реакции на инциденты в информационных сетях, использование интернета в криминальных целях и т.д. Подход к этой проблематике должен принципиально отличаться от традиционных для России практик с выраженным приоритетом роли специальных служб и вооруженных сил. Например, в вышеупомянутой Стратегии определено, что национальную безопасность обеспечивают именно армия и силовые структуры; практически идентичный посыл несет Доктрина.

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

В этой связи России необходима прежде всего *Стратегия кибербезопасности* верхнего, национального уровня, в которую будет входить список из конечного и конкретного списка задач, которые необходимо решать, а также сроки, к которым их надо решить. Нужны не общие слова, а конкретика. И исполнителями этой стратегии должны быть не только государственные органы и органы власти, а все задействованные и заинтересованные стороны, включая граждан в частном качестве. Зачатки этого подхода можно увидеть в недавнем документе по вопросам защиты объектов критической инфраструктуры[2]. Хотя и в нем, опять-таки, торчат уши вполне конкретных ведомств, а указанные ориентиры по срокам вызывают удивление. Так, появление в России системы обнаружения кибератак на критическую информационную инфраструктуру

запланировано только в период с 2017 до 2020 г., то есть через пять-восемь лет! Между тем уже два года назад вирус *Stuxnet* показал, какой ущерб может быть нанесен критической инфраструктуре лишь при помощи компьютерного кода. Следует помнить о том, что за прошедшее время арсенал кибероружия лишь увеличился и обогатился еще более сложными разработками. В то же время российская критическая инфраструктура сложнее и *разветвленнее* иранской, и уже поэтому нам следует быть готовыми к отражению подобных угроз сейчас, а не в среднесрочной перспективе.

ИНДЕКС БЕЗОПАСНОСТИ: *12 июля 2012 г. на сайте Совета безопасности РФ был опубликован очередной документ[2], посвященный вопросам защиты критической инфраструктуры в РФ. Входят ли вопросы безопасности критической инфраструктуры, включая инфраструктуру глобальной сети и ее российского сегмента, в круг приоритетов КЦ НДСИ? Какие угрозы безопасности инфраструктуры интернета существуют в РФ в настоящее время?*

КОЛЕСНИКОВ: Координационный центр обеспечивает работоспособность одного из главных критических элементов инфраструктуры Сети — системы доменной адресации. При этом специалисты КЦ стабильно демонстрируют стопроцентную доступность сервиса, что является одним из наших ключевых приоритетов.

Используя передовые технологические и методические подходы к построению географически распределенного сервиса, мы полностью исключили возможность злонамеренного влияния на сети извне и изнутри. В ближайшее время мы поднимем уровень доверия и защиты от подмены доменных ресурсов внедрением протокола DNSSEC [Domain Name System Security Extensions], обеспечивающего цепочки доверия между серверами DNS. Хотелось бы выразить надежду, что основные стратегические инфокоммуникационные системы в Российской Федерации используют столь же надежные методы и подходы.

Мы считаем, что проблематика кибербезопасности выходит далеко за пределы вопросов регламентирования доступности государственных служб и структур через интернет, равно как и сетевого обмена для обеспечения информационного взаимодействия госструктур. Напротив, доступность и безопасность электронных коммуникаций потребителей с банками и другими финансовыми учреждениями, системами интернет-торговли, системами электронных платежей, ведущими СМИ, социальными сетями, мультимедийными порталами и другими интернетсервисами вызывает большую озабоченность у общества, чем недоступность, например, сайта органа федеральной или муниципальной власти.

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

во-первых, отсутствие стратегических планов решения проблем кибербезопасности, отсутствие единой политики кибербезопасности России и опасность внутриведомственной борьбы в этой области;

во-вторых, отсутствие единого механизма управления вопросами кибербезопасности в России

в-третьих, низкая грамотность в области безопасного использования интернета, как дома, так и на работе;

в-четвертых, отсутствие законодательно закрепленных требований по обеспечению безопасности информационной инфраструктуры бизнеса, в том числе в критически важных областях, например в сфере инфокоммуникаций;

наконец, как следствие вышеперечисленного, отсутствие последовательной и прагматичной внешней политики в области управления интернетом, направленной на защиту конкретных интересов Российской Федерации в трансграничном киберпространстве.

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

КОЛЕСНИКОВ: Запуск домена *.рф* для Российской Федерации, а также иероглифической доменной зоны для КНР, арабской доменной зоны и других корневых доменов на национальных языках, а точнее алфавитах, отражает естественный процесс

эволюции адресного пространства интернета. При этом данный процесс не несет в себе фундаментальной тенденции потери единства глобальной сети.

Мы сталкиваемся с действием своеобразного фактора *Вавилона*, перенесенного в виртуальное пространство. Здесь важно помнить, что Рунет говорит по-русски со времен своего появления, и появление кириллических доменов лишь закрепляет языковую специфику российского сегмента Сети, не придавая ему каких-либо фундаментально новых качеств.

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

ИНДЕКС БЕЗОПАСНОСТИ: *Какова позиция Координационного центра в отношении недавно принятого закона 139-ФЗ? Какое техническое решение в блокировки контента, подпадающего под запрет в соответствии с положениями закона, Вы считаете оптимальным? В частности, как Вы оцениваете организационную, финансовую и техническую готовность российского интернет-сектора к широкому применению технологии DPI (deep packet inspection) с целью соблюдения положений 139-ФЗ?*

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

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

Думаю, что техническая готовность к исполнению закона будет обеспечена без особых проблем, так как у операторов есть возможность выбора методов фильтрации. Злоупотребления и неточность исполнения будут видны моментально. Но неблагодарное дело строить предположения, пока не появилась практика исполнения этого закона. В любом случае

необходимо будет смотреть на конкретные случаи применения закона в течение достаточно длительного времени, как минимум одного года. Очевидно, что оператором так называемого реестра *черного списка* будет Лига безопасного интернета, так как именно эта организация выступает локомотивом внесения ограничений в интернете для детей. И, по всей видимости, тема списков будет развиваться и, как мне кажется, следующий логичный шаг — это переоценка методов, используемых в *школьной* фильтрации.

Подход, который предписывает операторам *закрывать* доступ к ресурсам, предполагает использование оборудования, необходимого для глубокой проверки информационных пакетов (DPI) и обещает быть весьма затратным. Очевидно, что закон и его разработчики нуждаются в постоянной *обратной связи* с представителями интернет-сектора и экспертного сообщества, для корректировки слабых мест в тексте закона и повышения эффективности методов фильтрации. Необходимо также следить за случаями неизбирательного применения. Крайним примером здесь мог бы служить принцип блокировки противоправного контента по доменному имени. В случае с ФЗ-139 речь шла бы о полной остановке деятельности таких крупных сервисов и ресурсов, как *LiveJournal, YouTube, Facebook, Twitter* на территории Российской Федерации из-за единственной записи в аккаунтах кого-либо их пользователя, которая нарушала бы положения закона и не была бы удалена вовремя.

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

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

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

КИБЕРБИТВА ЗА РОДИНУ*

О государственной политике в сфере усиления безопасности в киберпространстве и возможных вариантах защиты пользователей от кибератак

А. Баулин

Реализация указа президента РФ, предусматривающего создание системы противодействия компьютерным атакам, может кардинально поменять климат в рунете. Пока ФСБ не раскрывает, как будет выполнять указ, мы решили рассмотреть возможные варианты защиты пользователей.

В 2012-м тема управления интернетом часто оказывалась в центре внимания — у ряда государств находились причины усилить контроль над сетью. В начале года США пытались протолкнуть у себя законопроект SOPA, позволяющий правообладателям жестко контролировать контент, потребляемый пользователями, и наказывать их, практически отменяя презумпцию невиновности. Заокеанским законодателям помешали собственная общественность и крупные местные компании (такие, как Google), активно протестовавшие против этого закона. Во время «арабской весны» Сирия отключила у себя доступ в интернет, желая предотвратить организацию повстанцев с помощью социальных сетей.

Россия, Китай и арабские государства стремятся усилить контроль над сетью внутри своих стран. Для этого они решили добиться изменения регламента Международного союза электросвязи — документа, определяющего полномочия государств по формированию правил работы интернета. В декабре им это удалось, но перемены оказались незначительными: главная роль в управлении мировой сетью по-прежнему принадлежит международной организации Internet Corporation for Assigned Names and Numbers (ICANN). Формально независимая, эта некоммерческая структура находится под влиянием США.

Однако российское правительство не отступилось от планов контроля над интернетом: на прошлой неделе был опубликован президентский указ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». В нем ФСБ предписывается создать подразделение, которое должно выполнить практически полный спектр работ по киберзащите российских ресурсов. В указе упоминаются все аспекты: от методики защищенности ресурсов до мониторинга состояния сети и разработки средств устранения последствий. В первую очередь обращается внимание на защиту ресурсов госорганов, а также на взаимодействие с операторами и компаниями, лицензированными на оказание услуг по информационной безопасности. По желанию владельцев в эту программу могут быть включены и другие информационные ресурсы.

После «Красного октября»

Насколько страшны кибератаки? Согласно отчету Symantec Cyber Crime Report — 2012, объем потерь мировой экономики от компьютерных преступлений составляет 110 млрд долларов в год. Если в стоимостном выражении доля России еще невелика, то по частоте атак мы в начале списка. А ведь не всегда хакеры портят данные и крадут деньги через интернет, они воруют государственные данные и блокируют доступ к сайтам — в таких случаях потери оценить сложно. Наталья Касперская, генеральный директор компании InfoWatch, специализирующейся на защите информации от утечек, связала появление указа с раскрытием сети зараженных компьютеров «Красный октябрь». Напомним: 14 января «Лаборатория Касперского» выявила сеть ПК в госорганах нескольких государств, включая Россию, с которых отсылалась информация в неизвестном направлении. И почти сразу появился указ президента № 31с (в компании Евгения Касперского утверждают, что к его разработке отношения не имеют).

Возникает вопрос: не является ли реальной целью указа не борьба с хакерскими атаками, а построение системы контроля за интернетом, в первую очередь за распространением оппозиционных настроений в соцсетях? Игорь Ашманов, управляющий партнер компании «Ашманов и партнеры», специалист в области искусственного интеллекта, разработки программного обеспечения и управления проектами, так не считает: «К построению “Великого русского брандмауэра” это отношения не имеет. У всех провайдеров уже лет десять стоит СОРМ-2* от ФСБ, и кому из “отцов русской демократии” он повредил? Мне кажется, возбуждающий фактор тут — само название спецслужбы. И никого не волнует, что, например, антивирусы — это

*Баулин А. Кибербитва за Родину / А. Баулин // Эксперт. - 2013. - № 4. - С. 46-49

замечательное средство не просто для контроля за гражданами, а хоть для захвата мира. Эта программа сидит в вашем устройстве на очень низком уровне и может сделать с операционной системой и железом что угодно. Добавим, что антивирус скачивает по закрытому протоколу сотни обновлений в день — не только данные, но и фактически самостоятельные программы». Правда, на наш взгляд, сам же Игорь Ашманов и упоминает причину, по которой при наличии СОРМ-2[1] требуется контроль за интернетом. Отвечая на вопрос, можно ли контролировать спам в западных соцсетях, он говорит: «Национальному государству может быть интересно душить в соцсетях какие-то массовые вбросы, призывы к беспорядкам или вражескую пропаганду. Однако сделать это можно только частично, блокированием всего сервиса целиком или сетевого протокола. Дело в том, что поисковики, социальные сети и твиттер быстро переходят на шифрованную связь с пользователем, на протокол HTTPS. Собственно, уже на 80–90 процентов перешли. Это значит, что в канале ничего увидеть нельзя, даже адреса конкретной страницы — вся жизнь социальной сети происходит в толстом клиенте, общающемся с сервером по закрытому протоколу. В результате можно либо запретить HTTPS, либо разрешать его до часа X, а потом выключать. Гипотетической альтернативой может стать установка следящих программ на пользовательском устройстве. Но это очень сложно логистически и технически».

Методы IT-борьбы

Как же бороться с информационными опасностями? Наиболее типичные компьютерные атаки: DDoS (перегрузка запросами сайтов с целью ограничения доступа к ним остальным пользователям), спам (почта и сообщения, не запрошенные пользователями и имеющие рекламный или агитационный характер), фишинговые ссылки и вредоносные программы, портящие и крадущие информацию, устанавливающие контроль за ПК пользователя.

Что касается DDoS, то Игорь Ашманов советует: «Если говорить об отражении DDoS-атаки, то эффективно с ней бороться не на атакуемом сайте, где канал узкий и производительность сервера ограничена, а, например, у провайдера, имеющего более широкий канал. Специальных продуктов для реализации такого подхода много — например, “Лаборатория Касперского” продает его уже несколько лет. В результате мы имеем большей частью техническую проблему: надо использовать надежные, пусть и дорогие, сетевые устройства, правильно настраивать сеть, применять специальное ПО». Ашманов подчеркивает, что важно не просто отразить атаку, а найти исполнителей и заказчиков: «Можно ли будет отследить источники атак? В принципе соответствующая инфраструктура, может быть, уже установлена у многих провайдеров. Гораздо интереснее, предполагается ли в рамках ФСБ выделить структуру для оперативно-розыскных действий: поиска и правового преследования хакеров после их выявления. Давно бы пора — мне кажется, что сетевой андерграунд слишком распоясался. И сетевые атаки не главная беда, больше урона приносят спам, трояны (программы, контролирующие ПК пользователя. — *“Эксперт”*), ботнеты (сети ПК, управляемые злоумышленником. — *“Эксперт”*), блокирование операционки, списывание денег».

От фишинговых ссылок, вредоносных программ, портящих информацию, и почтового спама защищают стандартные антивирусы в полных версиях класса Internet Secutity. Установив их, пользователь может вести вполне беззаботное существование.

А вот переписку в западных социальных сетях контролировать невозможно — выше мы уже упомянули, что весь трафик в них шифруется, посторонний не может прочитать сообщения. Если возникает необходимость противостоять политическому спаму, Игорь Ашманов наиболее логичным видит такой вариант: «Скорее всего, бороться в социальных сетях можно, только создавая “белковые средства”: специальные пропагандистские батальоны и автоматизированные рабочие места для них». Примеры таких подразделений, добавляет Ашманов, в мире уже есть.

Видимо, скоро появится еще один вид ПО, рассчитанный на борьбу с вредоносными программами, ворующими данные пользователя (в том числе номера и пароли кредитных карт или документы государственной важности) и отсылающими их хакеру. Если антивирус не смог остановить их, то могут пригодиться модифицированные системы типа DLP. «Еще год назад системы предотвращения утечек информации, DLP, разработкой которых занимается компания InfoWatch, не входили в список решений, предназначенных для защиты от кибератак, но с появлением “Красного октября” ситуация изменилась, — рассказывает Наталья Касперская. — Мы сейчас работаем над системой мониторинга, способной обнаруживать аномальную активность в сети, в том числе связанную с несанкционированным шифрованием конфиденциальной информации. Такая система призвана дать сигнал о соответствующем инциденте офицеру безопасности сети. Это уже не DLP в чистом виде, предстоит придумать название такой системе, которая может быть использована в том числе и для защиты информации в госструктурах». Современные антивирусные решения (имеются в виду системы полной защиты класса Internet Security), говорит Касперская, подобны стенам, возведенным вокруг компьютерной сети

организации. Но если раньше можно было полностью довериться стене, то теперь, когда вредоносные программы стали технически более сложными и совершенными и могут незаметно для внешней защиты проникнуть в сеть, необходимо научиться обнаруживать последствия их действий внутри периметра, ведь ущерб может быть колоссальным. А вот идея спрятать все госорганизации в закрытом сегменте сети Наталье Касперской кажется бесполезной: «Не думаю, что предложение некоторых экспертов выделить госорганизации в закрытую подсеть поможет. Наверное, это защитит от угроз определенного вида, но непременно будут созданы специализированные вредоносные программы для проникновения в этот изолированный периметр. Тем более что у каждого госучреждения свой набор аппаратных средств и программ — очень дорого обойдется стандартизировать такой зоопарк».

Можно предположить, что в будущей системе вышеперечисленные элементы будут объединены. Сайты защищены от DDoS-атак системами анализа трафика. Если хакеры попытаются обрушить их, заразив вирусами, то их атака будет предотвращена с помощью антивирусов класса Internet Security, которые будут установлены на персональные компьютеры сотрудников и серверы госорганизаций. Если же вредоносным программам удастся преодолеть антивирус до личных данных, то при попытке украсть файлы поднимут тревогу модифицированные системы DLP, которые сейчас разрабатываются. Единые стандарты для всех госорганизаций упростят организацию их защиты (за счет единообразности ПО) и понизят общую стоимость такой системы.

Внешняя или внутренняя защита?

Насколько реализуема такая система и есть ли ее аналоги в других странах? Илья Сачков, генеральный директор компании Group IB, помогающей МВД вычислять хакеров и собирать доказательства их преступлений, категоричен: «Очевидно, что подразумевается не техническая или не только техническая система. Половина пунктов указа говорит об организационных мерах, без которых создавать чисто техническую систему информационной безопасности в принципе неэффективно. По крайней мере, зарубежная практика показывает, что так никто не поступает». Один из экспертов по информационной безопасности, пожелавший остаться неназванным, отметил: «В указе речь идет о защите любых информационных ресурсов, находящихся на территории России. Это положение может относиться и к ресурсам, например, Министерства обороны, но они находятся вне компетенций ФСБ. Было бы логично создать при ФСБ уполномоченный орган, отвечающий за обеспечение национальной информационной безопасности в целом и координирующий данное направление в других организациях. Это поможет избежать возможного конфликта интересов. В США существует подобная система, и в каждом ведомстве есть структура, которая отвечает за свой участок».

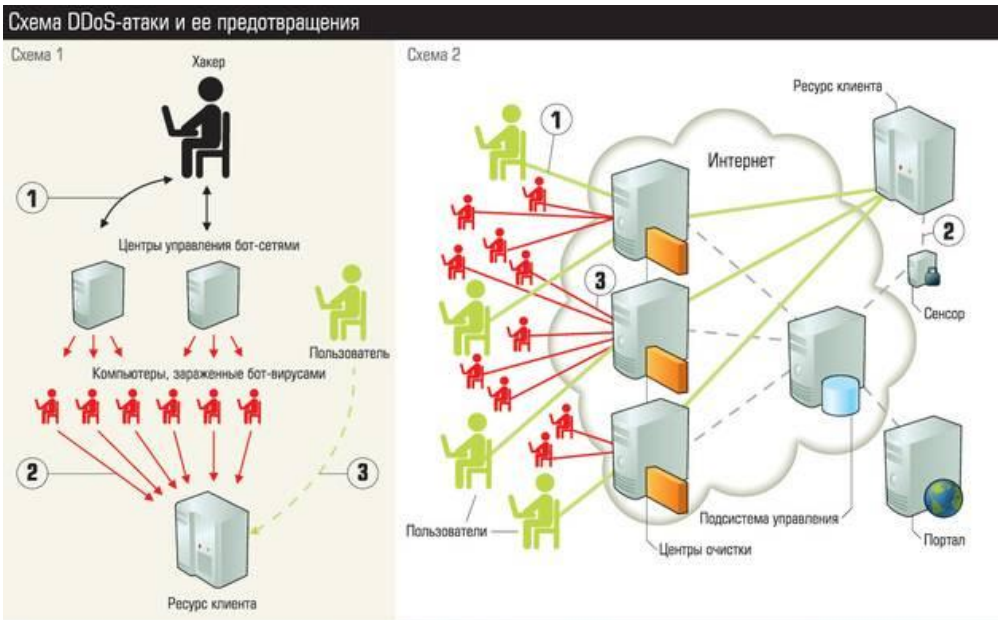
Отметим, что в ФСБ уже есть структура, которая могла бы взять на себя такие функции — ЦИБ (центр информационной безопасности, занимается антитеррористической деятельностью и защитой госинтересов в виртуальном пространстве), зачем же создавать новую? Наш источник в кругах, близких к ФСБ, сообщил, что указ был инициирован 8-м управлением ФСБ (бывшая служба ФАПСИ, отвечающая за безопасность каналов связи) и стал сюрпризом даже для других управлений этой организации. Однако есть и эксперты, считающие логичным создание единого надведомственного центра управления борьбы с киберпреступностью. Наталья Касперская отмечает: «Мера очень своевременная, такие органы противодействия киберугрозам на государственном уровне в других странах существуют уже давно. В частности, я знаю, что в Китае создан центр противодействия киберугрозам CNCERT. Компании, поставляющие в Китай продукцию для защиты от различных киберугроз, должны сертифицировать ее в CNCERT. Получившие сертификат обязуются предоставлять центру информацию обо всех совершенных на территории страны кибератаках».

Касперская полагает, что это правильный подход: хочешь защищать — докажи, что твоя продукция адекватна задачам. «Если бы я создавала систему противодействия, то сделала бы ее похожей на применяемую в Китае и Малайзии. Есть некий центр, который принимает вторичную информацию сразу от нескольких антивирусных компаний. В результате снижается вероятность ложных срабатываний на вредоносные программы. Кроме того, анализ первичного потока сообщений потребовал бы вовлечения в процесс сотни вирусных аналитиков, практически пришлось бы организовать еще одну антивирусную компанию. А если будет создан центр, достаточно парочки экспертов, которые станут анализировать и обобщать полученную информацию, и нескольких специалистов, занимающихся непосредственно поимкой киберпреступников. Учитывая, что такие функции уже в большой степени выполняются соответствующими ведомствами в МВД, можно использовать и имеющиеся ресурсы».

Спецы по пиковым нагрузкам

Но любые технические и организационные меры окажутся бесполезны, если инженеры не смогут реализовать систему, а пользователи не будут соблюдать меры безопасности. Поэтому в качестве главного средства борьбы с компьютерными атаками эксперты видят повышение профессионального и образовательного уровня. Так, Игорь Ашманов уверен, что DDoS-атаки случаются, но к «падениям» они приводят только при неграмотной настройке сайтов. И сайт ФСБ, и сайт госуслуг подвергаются атакам, а падает только ЖЖ (Livejournal.com), говорит Ашманов. Справедливости ради отметим, что и желающих зайти в ЖЖ больше, чем посетить сайт ФСБ, но вернемся к нашему разговору с Игорем Ашмановым. На вопрос, хватает ли России специалистов по пиковым нагрузкам, он ответил: «У нас мало всех ИТ-специалистов. Нам не хватает сотни ИТ-кафедр, десятков тысяч программистов и сисадминов в год. Так что и людей этой специальности тоже остро не хватает».

Илья Сачков видит еще одну проблему: часто хакеры уходят от ответственности, потому что судья не обладает соответствующими знаниями, позволяющими понять всю суть преступления. «С точки зрения взаимодействия с Управлением К — проблем нет, это оперативное подразделение, и они работу свою выполняют отлично, — говорит он. — Трудности начинаются, когда дела передаются в прокуратуру, суды. Хорошо было бы повысить уровень необходимых технических знаний сотрудников судов и прокуратуры, так как сейчас приходится очень много времени тратить на составление документов, поясняющих технологические термины, а то и суть самого компьютерного преступления, ведь юристы оперируют совершенно иными понятиями и терминами. Не хватает целевой программы и центров, которые обучат азам ИТ. Эксперты, конечно, могут разъяснить суть дела, но важен психологический момент: решение принимает судья. Он должен полностью разобраться в уголовном деле и сам принять обоснованное решение, а не полагаться только на заключение криминалиста. Если речь идет не просто о технической системе, а о национальной информационной безопасности, включающей необходимые правовые изменения, то это очень поможет».



[1]СОРМ-2 - система технических средств для обеспечения функций оперативно-розыскных мероприятий. Предусматривает возможность прослушивания разговоров граждан и протоколирования их деятельности в интернете.

КИБЕРБЕЗОПАСНОСТЬ И ПРОБЛЕМА ПОВЫШЕНИЯ КАЧЕСТВА УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ*

С.Е. Гришин, кандидат философских наук, доцент
С.Г. Седышев
(Саратовский государственный социально-экономический университет)

В условиях значительного, а порой и весьма избыточного объема информационных ресурсов в государственных учреждениях и организациях в полной мере о себе заявляют проблемы управления информацией и обеспечения ее защиты, причем ключом к успеху ИТ-безопасности является рациональное и качественное управление ею. Протоколы для стандартизации обработки информации и обеспечения ее безопасности сегодня имеются, во многих случаях они применяются при обработке информации, и все это свидетельствует об эволюции в сфере реализации требований кибербезопасности как в стратегическом, так и тактическом планах. Для защиты от попыток вторжения и предупреждения будущих угроз должны быть осуществлены инициативы, которые включают в себя разведывательные, оборонительные, наступательные, научно-исследовательские разработки, а также совершенствование государственно-частного партнерства. Задача обеспечения кибербезопасности органов государственной власти в условиях повсеместного внедрения информационных технологий решается путем улучшения управления информацией, для чего авторы предлагают ряд мер, которые должны быть положены в основу улучшения стратегии кибербезопасности на национальном уровне.

«Как ни странно это звучит, но объемы обмена информацией на государственном уровне сегодня явно завышены», – считает T. Sager, начальник отдела анализа уязвимостей и оперативной группы по информационному обеспечению Агентства национальной безопасности США [11]. И с его мнением трудно не согласиться. В условиях значительного, а порой и весьма избыточного объема информационных ресурсов в государственных учреждениях и организациях в полной мере обнаруживают себя проблемы управления информацией и обеспечения ее защиты, причем ключом к успеху ИТ-безопасности является рациональное и качественное управление информацией, что означает обеспечение возможности ее получения теми, кто в ней нуждается в интересах выполнения государственных функций. Но при этом массивы информации должны определяться стандартами, позволяющими применить инструменты, которые обеспечат оперативный анализ данных и сделают их доступными на санкционированной основе.

Набор протоколов для стандартизации обработки информации и обеспечения ее безопасности сегодня имеется. Во многих случаях эти протоколы применяются при обработке информации, что свидетельствует о тенденции в сторону принятия требований кибербезопасности как в стратегическом, так и тактическом планах.

Такие стандарты, регламентирующие совместимость программных продуктов, позволяют получать информацию из нескольких источников в различных форматах и делать ее доступной для пользователей [7]. Исследования позволяют утверждать, что, как правило, специалисты в крупных правительственных учреждениях обычно хорошо владеют тактикой реализации требований кибербезопасности, но они не так хорошо решают задачи управления информационными рисками на корпоративном уровне.

Процесс управления рисками должен начинаться в высших эшелонах государственного учреждения или организации, поскольку именно на первой линии защиты могут быть применены наиболее эффективные инструменты. «Однако оптимальной точки зрения на решение проблем информационной безопасности никогда не бывает, где бы ее ни пытались найти, – заявляет R. Team, – успехи на этом пути во многом определяются возможностью идентифицировать уязвимости сети или системы, но причины этих проблем и их окончательное решение находятся в совершенствовании практики управления IT-системой в начале ее жизненного цикла» [10].

*Гришин С.Е. Кибербезопасность и проблема повышения качества управления информацией / С.Е. Гришин, С.Г. Седышев // Вестник Саратовского государственного социально-экономического университета. - 2012. - № 1. - С. 202-206 (из фондов Научной электронной библиотеки *http://elibrary.ru*)

Есть несколько особенностей в обеспечении ИТ-безопасности. Если что-то произошло в сфере информационной безопасности сегодня, идентичное или близкое к тому, что случилось вчера, и это может повториться завтра, то чаще всего такую информацию персонал не доводит до тех, кто в ней нуждается (т.е. присутствует фактор латентности). Слишком часто сигналы и предупреждения о нарушениях информационной безопасности и инцидентах появляются значительно позже, что хорошо для последующей экспертизы, но обусловливает низкий уровень безопасности.

Рассмотрим возможные решения для более эффективного использования существующей информации, выявления уязвимостей, смягчения угроз и управления информационными рисками. Прежде всего, отметим, что не бывает простых решений для кибербезопасности, и вряд ли можно надеяться на расширение возможности государственных учреждений высокоэффективно использовать развивающиеся технологии для борьбы с эскалацией информационных рисков и угроз. Для этого необходима выработка согласованных руководств по безопасности информации на правительственном уровне, внедрение единой системы национальных стандартов и контроля, что поможет установить соответствующие уровни безопасности информации [5]. Руководство организаций должно больше внимания уделять непрерывному мониторингу ИТ-систем, большей их адаптации к применению новых средств защиты и более агрессивным кибератакам. Необходимо применять такие методы гибкой обороны, которые могут поднять расходы нападающих и ограничить последствия в случае успешной кибератаки, что способствует поддержанию эффективного управления информационными рисками. Настоящим фундаментом для этого должны стать стандартизация и совместимость [9].

Актуальность рассматриваемой проблемы во многом обусловлена устойчивым ростом количества кибератак на информационные системы органов государственной власти, что по-прежнему представляет собой потенциально разрушительные угрозы для информационных систем и осуществляемых операций. Все более возрастающая зависимость учреждений органов власти от применения автоматизированных систем для выполнения самых необходимых повседневных операций делают их уязвимыми для кибератак и информационных рисков. Таким образом, госучреждениям и организациям необходимо иметь эффективные программы информационной безопасности и управления информацией в целях защиты своих систем [9].

Ранее опубликованные материалы о развитии киберугроз в государственных информационных системах и инфраструктуре свидетельствуют, что такие риски и угрозы продолжают расти и развиваться [1; 4]. Они могут быть непреднамеренного или преднамеренного характера, целевыми или нецелевыми, поступать из различных источников, в том числе от преступников, террористов, и спецслужб иностранных государств, а также хакеров, недовольных сотрудников (внутренних саботажников).

Потенциальные злоумышленники используют самые различные приемы, имеющиеся в их распоряжении, которые могут значительно улучшить реализацию противоправных действий. Так, киберпреступники могут не находиться физически близко к своей цели, реализуемые ими атаки пересекают государственные и национальные границы, а кибернападающие нередко сохраняют анонимность [3; 8]. Кроме того, растущие взаимосвязи между информационными системами, Интернет и другие инфраструктуры представляют более широкие возможности для таких атак.

Информация об имевшихся инцидентах свидетельствует о наличии серьезных недостатков в системах безопасности, контроля над государственными информационными системами. Особую тревогу вызывают инциденты в сфере безопасности систем, обрабатывающих критически важную информацию. В частности, организации не всегда должным образом последовательно осуществляют политику аутентификации пользователей, чтобы предотвращать несанкционированный доступ к системам, не используют методы шифрования для защиты конфиденциальных и приватных данных и журналов, а также аудит и мониторинг состояния информационной безопасности.

Основная причина этих недостатков в том, что во многих организациях отсутствуют или не в полной мере и эффективно осуществляются имеющиеся политики и программы информационной безопасности, которые требуют постоянно осуществлять оценку и управление информационными рисками. Факты реализации киберугроз свидетельствуют в ряде случаев о слабой работе подразделений информационной безопасности и отдельных сотрудников. Разработка и внедрение политики безопасности и процедур, сопряженных с этим, повышение осведомленности в вопросах безопасности и обучение персонала, мониторинг

адекватности контроля уровню безопасности, осуществление соответствующих мер по исправлению положения – все это создает определенные возможности для повышения кибербезопасности.

Имеющаяся в стране нормативно-правовая и методическая база по вопросам информационной безопасности позволяет осуществлять координацию деятельности по обеспечению кибербезопасности, регламентации и четкого выполнения обязанностей службами информационной безопасности и специально выделенными для этого специалистами, наращивать и развивать потенциал для защиты критических инфраструктур и конфиденциальной информации.

Поддержание на высоком уровне информационной безопасности особенно важно для государственных учреждений, реализующих программы внедрения электронного правительства, что позволит обеспечивать конфиденциальность, целостность и доступность информации и информационных систем [2]. Неэффективное управление информационной безопасностью может привести к значительному риску для широкого круга органов государственного управления и активов. Примерами таких рисков могут быть следующие:

– потери ресурсов, платежей, налогов и сборов, которые могут быть похищены;

– имеющиеся ресурсы могут быть использованы в несанкционированных целях или для нападения на другие компьютеры;

– конфиденциальные данные о налогоплательщиках, социальном обеспечении, медицинские записи, документы интеллектуальной собственности, бизнес-информация и подобные данные могут быть неправильно раскрыты, несанкционированно просматриваться, копироваться в целях кражи или совершения других преступлений;

– нарушение операций, которые поддерживают критическую инфраструктуру, что особенно относится к деятельности правоохранительных органов, аварийно-спасательных служб, затрагивает интересы обороны;

– несанкционированное добавление, изменение или удаление информации в целях мошенничества или по другим корыстным соображениям;

– срыв реализации задач, поставленных перед государственным органом из-за возникших информационных инцидентов, что приводит к снижению уверенности граждан в способности органов власти проводить операции и выполнять свои обязанности.

Кратко рассмотрим причины и содержание этих угроз. Так, непреднамеренные угрозы могут быть вызваны невнимательными или неподготовленными сотрудниками, нарушением правил обновления программного обеспечения, технического обслуживания, отказов оборудования, что нарушает работу системы или повреждает базы данных.

Преднамеренные угрозы включают в себя целенаправленные и нецеленаправленные кибератаки. Целевыми можно назвать атаки, когда имеются групповые или отдельные нападения на конкретную систему или критическую инфраструктуру. Непреднамеренное нападение происходит тогда, когда цель атаки неопределенная, например когда происходит заражение вирусами, червями и другим вредоносным программным обеспечением, «гуляющим» по сети Интернет без какой-либо конкретной задачи.

Hacktivism относится к политически мотивированным кибератакам на общедоступные веб-страницы или серверы электронной почты путем перегрузки серверов электронной почты и взлома веб-сайтов с целью отправки политических сообщений. Недовольные инсайдеры, работая внутри организации, служат основным фактором компьютерных преступлений. Часто они не нуждаются в информации о методике компьютерных вторжений, так как их знание особенностей защиты системы позволяет им получить неограниченный доступ к информации, нанести повреждение системе или осуществить кражу данных из нее. Внутренние угрозы нередко связаны с персоналом подрядчиков (обслуживание и ремонт техники и т.п.).

Террористы стремятся разрушить, вывести из строя или использовать критически важные объекты инфраструктуры, чтобы угрожать национальной безопасности, привести к массовым жертвам, ослабить экономику страны, нанести ущерб общественной морали и доверию граждан к власти. Прогнозируется, что кибертеррористы в дальнейшем будут применять как традиционные методы атаки, так и киберугрозы, которые будут более технически совершенными за счет привлечения новых, более подготовленных участников. Кибератаки могут проводиться автоматически, на высокой скорости, одновременно может быть атаковано огромное количество жертв; растущая связь между информационными системами, через Интернет и другие инфраструктуры создает возможность для атак и разрушения каналов телекоммуникации, электроэнергии и других стратегически важных направлений.

С учетом того, что правительство, частный сектор и граждане в своей повседневной деятельности продолжают движение к активному использованию сетевых операций, поскольку цифровые системы имеют чрезвычайно широкие возможности, беспроводные системы становятся повсеместным явлением, а проектирование, производство, применение и обслуживание информационных систем перешагнуло государственные границы, угрозы в информационной сфере продолжают расти, становятся более целенаправленными и опасными.

Особо опасны эти инциденты из-за возможности утраты конфиденциальной информации, разглашения личной информации граждан, что потенциально влечет утрату конфиденциальности, совершению финансовых и иных преступлений. Имеющиеся факты кибератак и непреднамеренных инцидентов, связанных с критическими инфраструктурами, демонстрируют, что такие нападения могут иметь особо разрушительный характер.

Для защиты от попыток вторжения и предупреждения будущих угроз могут быть реализованы инициативы, которые включают в себя разведывательные, оборонительные, наступательные, научно-исследовательские разработки разработки, а также совершенствование государственно-частного партнерства. Кратко рассмотрим основные направления кибербезопасности.

1. Усиление анализа киберугроз и выработка мер предупреждения возможности их реализации. Атрибутами анализа киберугроз и их предупреждения могут быть:

– слежение за сетевой активностью для обнаружения аномалий;

– анализ информации и исследование аномалий с целью определения содержащихся угроз;

– своевременное предупреждение соответствующих должностных лиц в целях принятия мер по минимизации последствий угроз и выработки адекватного реагирования и ответа на угрозы, например, путем разработки и своевременного распространения широкого спектра уведомлений.

2. Улучшение кибербезопасности систем путем усовершенствования управления ИТ-инфраструктурой.

3. Укрепление способности оперативно восстанавливать деятельность из-за сбоев Интернета и кибератак посредством разработки планов, которые полностью отвечают всем установленным критериям в сфере ИТ-безопасности.

4. Сокращение организационной неэффективности эксплуатации ИТ-систем.

5. Повышение эффективности защиты внутренних информационных систем в учреждениях и организациях.

Таким образом, чтобы реализовать задачу обеспечения кибербезопасности органов государственной власти в условиях повсеместного внедрения информационных технологий путем улучшения управления информацией, необходимо разработать мероприятия, которые должны быть положены в основу улучшения стратегии кибербезопасности на национальном уровне.

1. Развитие национальной стратегии, которая ясно определит стратегические цели, цели и приоритеты в сфере защиты информации.

2. Установление ответственности органов власти за продвижение и наблюдение за реализацией национальной политики кибербезопасности.

3. Утверждение структуры управления реализацией политики и стратегии кибербезопасности.

4. Придание публичности проблемам кибербезопасности, формирование понимания в u1086 обществе их важности и серьезности.

5. Создание ответственной эксплуатационной организации для практического решения задач в сфере кибербезопасности.

6. Поддержание усилий общественных и частных структур в сфере кибербезопасности, выработка стимулов для реализации этой деятельности.

7. Сосредоточение внимания на исследовании глобальных аспектов кибербезопасности.

8. Полная реализация всех предусмотренных законом мер по пресечению умышленных и противоправных действий в киберпространстве.

9. Уделить больше внимания научным исследованиям кибербезопасности, включая рассмотрение того, как лучше координировать усилия власти и частного сектора по противодействию рискам и угрозам.

10. Наращивание работы по подготовке профессионалов для работы в сфере кибербезопасности.

11. Разработка для сотрудников органов власти алгоритмов действий в условиях реализации различных киберугроз.

Полагаем, что выполнение этих рекомендаций позволит надежно защитить информацию, накапливаемую и обрабатываемую информационными системами органов государственной власти, сделать ее менее уязвимой для рисков и угроз.

1. Джакер П.Т., Томпсон К.М. Электронное правительство в мире: уроки, проблемы, и будущие направления правительственной информации / пер. с англ. М., 2003.

2. Инструментальные средства для анализа рисков и управления рисками. URL:http://www//ftp.rmcs.department/ess/bss (дата обращения: 10.03.2010 г.).

3. Кононов А.А., Черешкин Д.С. Организация контроля безопасности региональной информационно-телекоммуникационной инфраструктуры // Информационное общество. 2002. Вып. 1.

4. Овчинников С.А., Гришин С.Е. Комплексный подход к рассмотрению теории управлением рисками при внедрении информационных технологий // Вестник СГСЭУ. 2011. № 2 (36).

5. Овчинников С.А., Гришин С.Е. Причины и условия неудач внедрения электронного правительства // Вестник СГСЭУ. 2011. № 4 (38).

6. Овчинников С.А., Гришин С.Е. Формирование культуры кибербезопасности в обществе – актуальная задача современности // Вестник СГСЭУ. 2011. № 3 (37).

7. Овчинников С.А., Семенов В.П. Проблемы стандартизации, совместимости и взаимодействия органов государственной власти, бизнес-процессов и граждан в условиях широкого внедрения информационных технологий // Информационно-коммуникационные технологии в сфере культуры: сб. мат. Международ. науч.-методич. конф. (19 – 24 сентября 2011 г., Саратов). Саратов, 2011.

8. Резолюции Генеральной Ассамблеи ООН от 30 января 2004 г. по докладу Второго комитета (A/58/481/Add.2)58/199. Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур от 23 января 2002 по докладу Третьего комитета (A/56/574) 56/121. Борьба с преступным использованием информационных технологий. URL:http://www:ifap.ru (дата обращения: 23.10.2010 г.).

9. EUROPA – Europe’s Information Society Thematic Portal. URL: http://www.europa.eu/ scadplus/ glossary/.htm (дата обращения: 25.10. 2011 г.).

10. URL: http://www.defense.gov/home/features/2010/0410_cybersec/docs/d10 230t.pdf (дата обращения: 25.10. 2011 г.).

11. URL: http://www//gcn.com/articles/2010/06/30/nist-releases-security-assessm-ent-guides (дата обращения: 25.10.2011 г.).

АДМИНИСТРАТИВНО-ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ*

И.М. Рассолов, доктор юридических наук, профессор
(Российский государственный торгово-экономический университет)

В настоящее время российские судебные органы испытывают определенные трудности при решении споров относительно правонарушений, связанных с Интернетом, а иногда и вовсе не готовы к рассмотрению дел данной категории.

Среди множества проблем судебной практики по этим делам можно выделить две ключевые:

1) сложность определения круга лиц, привлекаемых к юридической ответственности и обязанных компенсировать моральный вред и материальный ущерб пострадавшему;

2) фиксация (собирание, представление) доказательств, их допустимость и достоверность. Процесс распространения информации в Интернете в этом случае можно описать как процесс, в котором помимо самого автора участвуют еще два субъекта (лица): собственник сайта (сетевого информационного ресурса) и собственник сервера (хост-провайдер). Следовательно, потенциальными ответчиками могут являться как хост-провайдеры (разместившие информационный ресурс на своем сервере), так и собственники информационных ресурсов.

Возможность анонимного присутствия в Сети позволяет скрыть подлинные имена автора, источника и лица, разместившего информацию. Примером могут служить так называемые гостевые книги, которые открываются на сайтах для выражения мнения посетителей или выступают в качестве одной из форм изучения общественного мнения. Естественно, что каждый последующий посетитель имеет возможность познакомиться с мнением предыдущего. Найти автора подобного «мнения» сложно.

Информационное наполнение и использование сети Интернет в коммерческих и некоммерческих целях осуществляется посредством услуг организаций, обеспечивающих доступ к сети Интернет.

Провайдер — специализированная организация, оказывающая услуги по доступу в Сеть, размещению и передаче информации в Сети.

В настоящее время провайдер — это основной поставщик услуг в сети Интернет.

Среди базовых услуг, которые предоставляют провайдеры, можно выделить: организацию доступа в сеть Интернет и предоставление свободного дискового пространства на сервере для размещения сайта, принадлежащего другому лицу (хостинг).

С точки зрения права, чтобы стать пользователем Сети, необходимо заключить с провайдером договор об оказании услуг по доступу в Сеть (т.е. установить с провайдером необходимые интернет-отношения). Для сеанса доступа в Интернет провайдер предоставляет пользователю IP-адрес (число, состоящее из четырех частей), который позволяет однозначно идентифицировать каждый компьютер в Интернете. IP-адрес необходим для маршрутизации запросов пользователя, когда с этого адреса на сервер провайдера поступает запрос пользователя, — компьютер провайдера осуществляет поиск в сети Интернет полученных данных и отправляет найденную информацию на IP-адрес пользователя. Отсюда возникло определение провайдера как информационного посредника.

Информационное наполнение сети Интернет осуществляется посредством заключения договора хостинга. По своей правовой природе договор хостинга схож с договором аренды: провайдер за определенную плату предоставляет лицу свободное дисковое пространство на своем сервере, а указанное лицо размещает на нем сайт. Согласно ст. 3 Федерального закона от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» провайдер хостинга — это лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет.

Нужно отметить, что действия информационных провайдеров по оказанию услуг характеризуются следующими чертами: провайдер не инициирует информационное отношение, не выбирает содержание передаваемой информации и ее получателя, не влияет на содержание

*Рассолов И.М. Административно-правовые проблемы обеспечения кибербезопасности / И.М. Рассолов // Государственный аудит. Право. Экономика. - 2012. - № 4. - С 166-173

информации, однако он хранит информацию только в пределах времени, определяемого техническими стандартами и протоколами исходя из нужд передачи информации[1].

Указанная многомерность отношений, а также тот факт, что провайдер имеет техническую возможность в любой момент воздействовать на информационные отношения своих пользователей, определили появление института ответственности провайдеров.

Изучение законодательства разных государств показало, что в них проблема административной ответственности провайдеров решается по-разному. Причем здесь можно выделить три основных подхода к решению данной проблемы:

1) провайдер несет ответственность за все действия пользователей вне зависимости от наличия у него как у субъекта права знания о совершаемых действиях;

2) провайдер не несет ответственности за пользователей в том случае, если выполняет определенные условия, связанные с характером предоставления услуг и взаимодействием с субъектами информационного обмена и лицами, чьи права нарушаются действиями пользователей;

3) провайдер не отвечает за действия пользователей.

В Китае и странах Ближнего Востока, например, используется первый подход, в Европе — второй. Так, в Европейской директиве по электронной коммерции[2] от 28 февраля 2000 г. (разд. 4, ст. 12–15) проработано наиболее детально решение проблемы указанного вида юридической ответственности.

Директива устанавливает, что провайдер не несет ответственности за передаваемую информацию в случае, если он не инициирует ее передачу, не выбирает получателя информации и не влияет на целостность передаваемой информации. При этом допускается временное хранение передаваемой информации для осуществления необходимых технических действий по ее передаче.

Утверждается, что провайдер не несет ответственности за действия пользователей при предоставлении услуг хостинга, если он не был осведомлен об их противозаконной информационно-правовой деятельности и после получения информации об этом прекратил размещение или доступ к информации. Аналогичное положение устанавливает и Закон об информации, информационных технологиях и о защите информации от 27 июля 2006 г. (ст. 17 Закона).

В настоящее время в ряде стран мира приняты предметные законы, касающиеся института ответственности провайдеров. Так, в шведском законе, регулирующем ответственность владельцев досок объявлений (Act (1998:112) on Responsibility for Electronic Bulletin Boards), устанавливается, что таковые обязаны удалять сообщения третьих лиц в том случае, если содержащаяся в них информация нарушает ряд норм уголовного и гражданского законодательства (в части авторского права).

Похожая на европейскую, но менее детальная схема ответственности при нарушении авторских прав определена в американском Digital Millenium Copyright Act (DMCA)[3], принятом в 1998 г. В Англии действует Defamation Act[4], принятый в 1996 г., который регулирует ответственность интернет-провайдеров за достоверность размещаемой на их сайтах информации.

До сегодняшнего момента в российском законодательстве четко не были определены механизмы привлечения к ответственности провайдеров за размещение на обслуживаемых ими сайтах недостоверной информации, а также не установлена возможность предъявления к ним претензий за качество размещаемой информации.

Однако некоторую ясность в данный вопрос внесли последние поправки в законодательство о защите детей от информации, причиняющей вред их здоровью и развитию.

В частности, Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации»[5] предусматривает введение новой статьи 15.1, согласно которой вводиться Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющий идентифицировать сайты. Сайты, внесенные в данный реестр, будут заблокированы. Распространение вредной информации, размещаемых на этих электронных площадках, в Российской Федерации будет запрещено. Закон впервые устанавливает четкие процедурные нормы для блокирования вредного контента:

1. Создание, формирование и ведение реестра будет осуществляются федеральным органом исполнительной власти, выполняющим функции по контролю и надзору в сфере средств массовой информации (Роскомнадзором).

2. Роскомнадзор может привлечь к формированию и ведению реестра оператора реестра — организацию, зарегистрированную на территории Российской Федерации.

Основаниями для включения в реестр сведений будут являются:

а) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном

Правительством Российской Федерации, в отношении распространяемых посредством сети Интернет;

б) материалы с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

в) информация о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

г) информация о способах совершения самоубийства, а также призывов к совершению самоубийства;

д) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено.

Причем решение о включении в реестр может быть обжаловано владельцем сайта в суд в течение трех месяцев со дня принятия такого решения.

Процедура блокировки будет выглядеть следующим образом.

В течение суток с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта и уведомить его о необходимости незамедлительного удаления вредной интернет-страницы.

В течение суток с момента получения от провайдера хостинга уведомления о включении доменного имени в реестр владелец сайта обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта провайдер хостинга обязан ограничить доступ к такому сайту в сети Интернет в течение следующих суток.

В случае непринятия провайдером хостинга и (или) владельцем сайта необходимых мер сетевой адрес, позволяющий идентифицировать сайт в российских зонах Интернета, включается в реестр.

В течение еще одних суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети Интернет, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети обязан ограничить доступ потребителей к такой информации.

Вместе с тем, как мы считаем, необходима еще более детальная и четкая проработка законодательного разрешения в отношении ответственности информационных посредников, причем как в России, так и в странах СНГ. Это также касается возможного манипулирования и неоправданного отсечения «неудобных» сайтов также со стороны официальных властей. Тем более что последние судебные процессы только подтверждают актуальность подобной постановки вопроса.

На наш взгляд, изменения и дополнения в российское законодательство должны вноситься по принципу, в соответствии с которым провайдер должен нести ответственность за качество информации, размещаемой на его сервере, в случае, если:

1) данная информация размещалась по его инициативе и/или за его счет;

2) провайдер был осведомлен или имел возможность быть осведомленным о содержании информации, размещаемой на его сервере;

3) преднамеренные или непрофессиональные (противоречащие профессиональной подготовке, работе и возможности) действия провайдера повлекли размещение незаконной информации на его сайте.

Таким образом, ответственность провайдера наступает в зависимости от наличия его вины в размещении информации, нарушающей права третьих лиц.

Бремя доказательства отсутствия вины провайдера следует возложить на самого провайдера, который должен привлекаться в судебный процесс в качестве ответчика, а в случае отсутствия его вины ненадлежащий ответчик должен заменяться лицом — собственником информационного ресурса (провайдер остается в процессе в качестве третьего лица).

Такой механизм привлечения к ответственности будет вполне оправдан, если учесть, что фактически информация размещена на дисковом пространстве сервера, принадлежащего провайдеру (т.е. источник противоправной информации — компьютер провайдера).

В этом случае провайдеры сами будут заинтересованы в более тщательной проверке информации.

Необходимо законодательно закрепить право провайдера по результатам проверки:

— или блокировать информацию, для выявления противозаконности содержания которой не требуется специальных знаний;

— или информировать компетентные органы о наличии сомнительной информации для более тщательной и компетентной проверки.

На наш взгляд, потенциал провайдера необходимо использовать в интересах упрощения процедуры по сбору доказательств в судебном процессе.

Кроме того, необходимо обязать провайдеров регулярно копировать информацию с лог-файла[6], бережно хранить и предоставлять ее при первом требовании заинтересованных и компетентных государственных органов.

Обобщая сказанное, можно утверждать, что проблема ответственности провайдеров — это особенно острая и насущная проблема государственной информационной политики, но и вообще в сфере государственной безопасности.

Исследование показало, что заметные осложнения вызывают информационные отношения, возникающие в кибернетическом пространстве и отягощенные иностранным элементом. Они имеют место, когда сделка в электронной форме либо заключается гражданами разных государств, либо ущерб в результате использования сайта причинен на территории иностранного государства, либо информация, размещенная на сайте, нарушает законы иностранного государства об охране прав интеллектуальной собственности.

На практике довольно часто распространена ситуация, когда потребитель информации, собственник информационного ресурса и хост-провайдер являются гражданами разных государств. При возникновении между сторонами судебного разбирательства встают следующие проблемы:

1) юрисдикции какого государства подчинено правоотношение (т.е. суд или компетентный орган какого государства вправе рассматривать дело);

2) право какого государства подлежит применению (традиционно в международном частном праве используются коллизионные привязки для определения применимого права — «закон места нахождения», «закон места заключения», «закон места причинения» и т.д. Однако в настоящее время они все более приобретают совершенно иное звучание в связи с Интернет-отношениями и используются в сочетании с таким критерием, как «место нахождения сервера»).

Как правило, у субъектов информационных отношений, осложненных иностранным элементом, есть возможность выбрать применимое право и место рассмотрения спора. Однако не во всех случаях этот способ будет эффективен. Стороны не всегда смогут по объективным или субъективным причинам совершить свой выбор, например просто не договориться.

Правовое регулирование в данной новой области только начало складываться, и пути его развития пока еще не определены.

В любом интернет-споре с иностранным элементом в первую очередь возникает вопрос о том, в суд какого государства подать иск.

Механизмы и процедурные нормы, по которым решаются подобные вопросы, в рамках каждой национальной юрисдикции различаются и имеют специфику. По процессуальным вопросам в международном частном праве традиционно применяется правило lex fori, по которому каждый суд применяет свое собственное право. В разных государствах правила определения международной подсудности имеют характерные черты и особенности. Тем не менее национальность или место нахождения ответчика — основной критерий, которым руководствуются суды при решении вопроса о наличии своей компетенции рассматривать интернет-спор.

Основанием такого правила исторически выступает фактор физического присутствия или физической досягаемости ответчика для суда. Однако бурное развитие высоких технологий, сложность определения места и времени совершения сделки (интерактивного обмена данными) уже не позволяют этому условию играть решающую роль. Экстерриториальность Сети дает возможность преступнику нарушать законы государства без физического нахождения на его территории (например, последние события вокруг пирамиды МММ-2012 в Республике Беларусь). Следовательно, суду для надлежащего обеспечения правопорядка на своей территории необходимо расширять правила юрисдикции и за основу брать уже не закон ответчика, как считает Е. Леанович, а «фактическую связь спорного отношения с государством суда»[7].

В этой связи интересна практика судов США (темпы развития американского рынка телекоммуникаций — основная причина большого опыта рассмотрения подобных интернет-споров в судах США).

До настоящего времени в США основным принципом решения юрисдикционных проблем являлась так называемая персональная юрисдикция (personal jurisdiction), в соответствии с которой суд обладает компетенцией по рассмотрению интернет-спора в отношении физического или юридического лица, если оно физически присутствует на его территории. Однако сегодня этот принцип дополнен, а порой напрямую заменен принципом минимальных контактов, т.е. связь ответчика с определенной территорией может служить оправданием для юрисдикции суда этой

территории, и само физическое пребывание (статус резидента) ответчика не является определяющим условием юрисдикции американских судов[8].

Во многих штатах критерии выявления минимальных контактов закреплены законами «длинной руки» (long arm statutes). В этом случае можно вести речь об экстерриториальности закона, распространении его действия на граждан и вне пределов того штата, в котором был издан данный закон. Среди подобных критериев следует особо выделить различные юридические факты, в основном действия. Например, факт заключения сделки (договор поставки товара, оказания услуг); владение и пользование недвижимостью; наличие постоянного счета в американском банке, по которому производится расчет с кредитором; причинение имущественного вреда на соответствующей территории. Поэтому в интернет-спорах американские суды признают наличие своей юрисдикции, принимая во внимание только существование определенных связей правоотношения с территорией США даже в том случае, если ответчик не является резидентом этой страны.

Простое размещение на сайте информации о товарах и услугах может быть рассмотрено как основание для вывода о наличии юрисдикции (если, например, лицо не ограничивает доступ к размещаемым в Интернете сообщениям резидентам США или размещаемая информация доступна на английском языке).

Изучение показало, что в европейских странах вопросы международной подсудности решаются в основном исходя из критерия физической досягаемости ответчика. Условно можно выделить три основные системы определения подсудности:

1) по закону гражданства (Франция);

2) по закону домицилия (Германия) и

3) по признаку фактического присутствия ответчика на территории страны суда (Великобритания).

Кроме того, позитивное право и судебная практика европейских государств предусматривают возможность судебного разбирательства в отношении субъектов (лиц), не являющихся гражданами и не находящихся на их территории. Это происходит в том случае, когда спорное правоотношение тем или иным образом связано с судом государства[9]. Например, в качестве таких критериев связи может выступать нахождение имущества, факт заключения сделки или причинения вреда ответчиком на территории государства суда. Однако каким образом специфика правоотношений в Интернете может повлиять на изменение основных правил определения подсудности в европейских государствах, судить пока сложно.

В этой связи можно предложить решение проблемы определения юрисдикции путем межгосударственного согласования применяемых критериев. Для этого возможны следующие способы:

1) заключение международного соглашения об определении вопросов юрисдикции в отношении деятельности с использованием сети Интернет, в котором необходимо определить критерии отнесения к юрисдикции государства для каждого распространенного типа отношений;

2) частичное устранение проблем путем унификации материального законодательства. Если однородные интернет-отношения будут защищаться в различных государствах в одинаковой степени, выбор юрисдикции будет не принципиален.

В этой сфере также важно развивать международно-правовое сотрудничество, в том числе и по линии правоохранительных и судебных органов.

Международное частное право и международное уголовное право уже сегодня предлагают многочисленные решения по вопросу правового регулирования отношений, возникающих, изменяющихся и прекращающихся в информационной сфере. Действительно, общие механизмы выдачи преступника иностранному государству и международной правовой помощи в сфере уголовного права уже сегодня могут применяться в отношении преступлений, совершенных в электронной среде Интернета.

Так, в Европе давно уже действуют соглашения о выдаче преступников иностранному государству. Некоторые из них Россия подписала и ратифицировала. Среди них, например, Европейская конвенция о выдаче[10] от 13 декабря 1957 г., Европейская конвенция о взаимной правовой помощи по уголовным делам[11] от 20 апреля 1959 г. До недавних пор не существовало детального договора между Россией и США по данному вопросу. Действовало лишь Соглашение между двумя странами о порядке исполнения судебных поручений от 22 ноября 1935 г. (в форме обмена нотами)[12]. Только 17 июня 1999 г. был подписан Договор между РФ и США о взаимной правовой помощи по уголовным делам, который был ратифицирован Федеральным законом от 3 ноября 2000 г.[13] Развивая это сотрудничество, следует в ближайшее время подписать еще один специальный договор между Россией и США о взаимной выдаче преступников, который затрагивал бы и сферу Интернета. Это окажет положительное воздействие на рынок интернет-услуг.

Российским юристам еще предстоит выработать свою точку зрения по проблеме юридической ответственности лиц, совершивших правонарушения в кибернетическом пространстве, анализируя гл. 28 УК РФ и другие национальные нормы права. Рекомендация Совета Европы № R (95) 13 относительно проблем уголовных процедур, связанных с технологией обработки информации[14], могла бы послужить базой для такой правовой работы[15]. Следует подвергнуть всестороннему анализу этот нормативный акт в целях совершенствования отечественной правоприменительной практики. Вероятно, соответствующие законодательные изменения могли бы быть успешно внесены и в другие международные акты. Скорейшее присоединение России к Конвенции о киберпреступности решило бы многие проблемы в сфере административного и уголовного права, а также способствовало бы выработке понятийного аппарата информационного права. Тем более, как нам представляется, теперь это вопрос лишь времени[16].

[1]См.: Наумов В.Б. Право и Интернет: очерки теории и практики. М.: Книжный дом «Университет», 2002. С. 55–67; Он же. Проблемы ответственности информационных провайдеров // Третья Всероссийская конференция «Право и Интернет: теория и практика». 28–29 ноября 2000 г. М., 2000. С. 77–79.

[2]Директива 2000/31/ЕС Европейского парламента и Совета о некоторых правовых аспектах услуг информационного общества, в том числе электронной коммерции, на внутреннем рынке (вступила в силу 8 июня 2000 г.). // Шамраев А.В. Правовое регулирование информационных технологий (анализ проблемы и основные документы). М.: Статут; Интертех; Издательская группа «БДЦ-пресс». 2003. С. 317–327.

[3]См.: Marcia K. Wilbur. DMCA: The Digital Millenium Copyright Act. Lincoln (Nebraska): Writers Club Press. 2001. 268 p. URL: http://www.copyright.gov/legislation/dmca.pdf

[4]Clare Sandford, Fiona Boyle. Defamation Act 1996: The New Law (Impact Series). Newcastle upon Tyne: Northumbria Law Press. 1997. 102 p. URL: http://www.opsi.gov.uk/acts/acts1996/1996031.htm

[5]Собрание законодательства РФ. 2012. № 31. Ст. 4328.

[6]Лог-файл (от англ. log files) представляет собой специальный файл, содержащий системную информацию о работе сервера и сведения о действиях пользователей: дату и время визита пользователя; IP-адрес компьютера пользователя, а также иные настройки. Исследуя лог-файлы, можно получить сводные цифры активности потребителей интернет-услуг, изучить закономерности поведения различных групп, их предпочтения, интересы.

[7]Леанович Е.Б. Проблемы правового регулирования Интернет-отношений с иностранным элементом // Белорусский журнал международного частного права и международных отношений. Минск. 2000. № 4. С. 39–44.

[8]Там же.

[9]Богуславский М.М. Международное частное право. М.: Юристъ, 2002. С. 398–437.

[10]Федеральный закон от 25 октября 1999 г. № 190-ФЗ «О ратификации Европейской конвенции о выдаче, Дополнительного протокола и Второго дополнительного протокола к ней» // СЗ РФ. 1999. № 43. Ст. 5129. Конвенция вступила в силу для Российской Федерации 9 марта 2000 г. Официальный перевод текста Конвенции на русский язык см.: СЗ РФ. 2000. № 23. Ст. 2348.

[11]Федеральный закон от 25 октября 1999 г. № 193-ФЗ «О ратификации Европейской конвенции о взаимной помощи по уголовным делам и Дополнительного протокола к ней» // СЗ РФ. 1999. № 43. Ст. 5132. Конвенция вступила в силу для Российской Федерации 9 марта 2000 г. Официальный перевод текста Конвенции на русский язык см.: СЗ РФ. 2000. № 23. Ст. 2349.

[12]Соглашение в форме обмена нотами между Союзом Советских Социалистических Республик и Соединенными Штатами Америки о порядке исполнения судебных поручений (Москва, 22 ноября 1935 г.) // Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. IX. М., 1938. С. 79–84.

[13]См.: Федеральный закон «О ратификации договора между Российской Федерацией и Соединенными Штатами Америки о взаимной правовой помощи по уголовным делам» от 3 ноября 2000 г. // СЗ РФ. 2000. № 45. Ст. 4401.

[14]URL: https://wcd.coe.int/ViewBlob.jsp?id=538299&SourceFile=1

[15]См. более подробно: Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие / под ред. Ю.В. Гаврилина. М.: Юридический институт МВД РФ. 2003. 245 с.

[16]Сначала Россия приняла решение подписать Конвенцию с заявлением. Президент РФ подписал распоряжение от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности» // СЗ РФ. 2005. № 47. Ст. 4929. Однако в марте 2008 г. Россия отказалась поставить свою подпись под этим документом. См.: Распоряжение Президента РФ от 22 марта 2008 г. № 144-рп «О признании утратившим силу Распоряжения Президента РФ от 15 ноября 2005 г. №557-рп «О подписании Конвенции о киберпреступности».

ГОСУДАРСТВЕННЫЕ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ*

1. Введение

Долгое время общественное благосостояние и экономическая стабильность опирались на надежную работу сетей передачи данных и вычислительных сервисов. На функционирование ключевых информационных систем общего пользования оказывают влияние многие факторы: Интернет-атаки, нарушения, вызванные физическим воздействием, выход из строя программного и аппаратного обеспечения, человеческие ошибки. Перечисленные явления наглядно демонстрируют, насколько современное общество зависит от стабильной работы информационных систем. Подобная мысль повторяется и в немецкой стратегии кибербезопасности: “Обеспечение доступности киберпространства, а также целостности, достоверности и конфиденциальности информации в киберпространстве стало одной из важнейших проблем 21-го столетия. Именно поэтому защита киберпространства становится главной задачей государства, экономики и общества, как на государственном, так и на международном уровне”.[1]

На некоторых собраниях[2] Европейской комиссии особо отмечалась важность сетевой и информационной безопасности и необходимость создания единого Европейского Информационного Пространства. В существующих и продвигаемых правках нормативно-правовой базы[3], а также на последних собраниях Европейской комиссии, посвященных защите ключевой информационной инфраструктуры[4] (CIIP), предлагаются практические меры и регулятивные нормы по усилению безопасности и надежности[5] сетей общего пользования.

Кибербезопасность все чаще рассматривается, как стратегическая проблема государственной важности, затрагивающая все слои общества. Государственная политика кибербезопасности (national cyber security strategy - NCSS) служит средством усиления безопасности и надежности информационных систем государства. В стратегии к проблеме кибербезопасности применяется высокоуровневый и нисходящий подход: выдвигается ряд государственных целей и приоритетов, которые необходимо достичь за определённый промежуток времени. Фактически, стратегия представляет собой модель решения задачи кибербезопасности внутри государства.

Для того чтобы поддержать страны - члены Евросоюза в важной миссии по разработке и поддержке государственной политики кибербезопасности, ENISA разрабатывает специальное руководство[6] (Good Practice Guide). В руководстве даются рекомендации, а также передовая практика по разработке, внедрению и поддержке в актуальном состоянии стратегии кибербезопасности.

В настоящем документе представлены предварительные результаты, полученные при работе над руководством. Документ включает в себя краткий анализ текущего состояния стратегий кибербезопасности стран - членов Евросоюза, а также других стран; затем определяются общие черты и различия в стратегиях; и в самом конце приводится ряд выводов и рекомендаций.

2. Развитие стратегий кибербезопасности в странах-членах Евросоюза

Первые стратегии кибербезопасности начали появляться в начале предыдущего десятилетия. Одной из первых стран, которые стала воспринимать кибербезопасности, как вопрос государственной важности были Соединенные Штаты Америки. В 2003 году в США опубликована Национальная стратегия безопасности в киберпространстве[7] (National Strategy to Secure Cyberspace). Документ являлся частью более общей Стратегии обеспечения национальной безопасности (National Strategy for Homeland Security), созданной в ответ на террористические атаки 11 сентября 2001 года.

В последующие годы по всей Европе начали распространяться планы мероприятий и стратегии, призванные решить подобную задачу. В 2005 году Германия принимает Государственный план защиты информационной инфраструктуры[8] (National Plan for Information Infrastructure Protection – NPSI). В следующем году Швеция разрабатывает Стратегию усиления безопасности Интернета в Швеции (Strategy to improve Internet security in Sweden). Вслед за крупной кибератакой в 2007 году Эстония стала одной из первых стран-членов Евросоюза, опубликовавшей в 2008[9] году широкую государственную стратегию кибербезопасности. С тех пор в этой сфере на государственном уровне была проделана большая работа, и в последние четыре года десять стран-членов Евросоюза опубликовали свои государственные стратегии кибербезопасности. Краткое описание стратегий приводится ниже.

---

*Государственные стратегии кибербезопасности / Европейское агентство по сетевой информационной безопасности (ENISA) // Опубликовано 4 сентября 2012 года на сайте информационного портала по безопасности SecurityLab.ru *http://www.securitylab.ru/*

Некоторые страны, входящие в Евросоюз, в настоящий момент разрабатывают стратегии, которые уже близки к завершению. Кроме того, у нескольких стран-членов есть неофициальные или неформальные стратегии.

Эстония (2008): Эстония придает особое значение необходимости защиты киберпространства в целом и ставит в центр внимания безопасность информационных систем. Рекомендуемые меры носят гражданский характер и основываются на правовом регулировании, обучении и сотрудничестве.

Финляндия (2008): В основе стратегии лежит понимание кибербезопасности как проблемы экономического характера, тесно связанной с развитием финского информационного общества.

Словакия (2008): Обеспечение информационной безопасности рассматривается в качестве необходимого условия нормального функционирования и развития общества. Поэтому цель стратегии – служить прочным фундаментом для защиты информации. Стратегия направлена как на предотвращение угроз, так и на обеспечение готовности и устойчивости средств их предотвращения.

Чешская Республика (2011): Ключевые цели стратегии кибербезопасности включают в себя защиту информационно-коммуникационных систем от уязвимостей, которым эти системы подвергнуты, и уменьшение потенциального ущерба от атак на системы. Основной фокус стратегии приходится на проблемы свободного доступа к информационным сервисам, целостности и конфиденциальности данных в киберпространстве Чешской Республики. Стратегия хорошо согласуется с другими нормативно-правовыми документами Чешской Республики.

Франция (2011): Франция ориентируется на то, чтобы информационные системы были способны противостоять событиям в киберпространстве, которые могут отрицательно повлиять на доступность, целостность и конфиденциальность информации. Франция делает упор на технические средства защиты информации, борьбу с киберпреступностью и установление киберзащиты.

Германия (2011): Стратегия Германии закладывает основу для безопасности критически важных информационных систем. Германия сосредоточена на предотвращении и уголовном преследовании кибератак, а также на предотвращении выхода из строя IT-оборудования, вызванного случайными факторами. В особенности последнее касается критически важных информационных систем. В стратегии анализируется, нужно ли производить дополнительные действия (и если да, то где именно) по защите IT-систем путем предоставления основных функций безопасности, сертифицированных государством, а также поддержкой малого и среднего бизнеса посредством создания новой рабочей группы.

Литва (2011): Литва ориентируется на определение целей и мероприятий, направленных на развитие оборота электронной информации, а также обеспечения ее конфиденциальности, доступности и целостности в киберпространстве. Кроме того, стратегия Литвы направлена на защиту персональных данных, телекоммуникационных сетей, информационных систем и критически важных инфраструктур от нарушения безопасности и кибератак. В стратегии также определены мероприятия, реализация которых будет гарантировать полною безопасность работы в киберпространстве.

Люксембург (2011): Осознавая уязвимость информационно-коммуникационных технологий, стратегия утверждает, что важнее всего – общественная и экономическая безопасность. В стратегии также отмечается важность информационно-коммуникационных технологий для экономического роста, отдельных граждан и общества в целом. Стратегия работает по пяти направлениям: защита ключевой информационной инфраструктуры и своевременная реакция на инциденты безопасности; модернизация нормативно-правовой базы, государственное и международное сотрудничество; обучение и информирование; продвижение стандартов.

Голландия (2011): Голландия, с одной стороны, стремится к безопасным и надежным информационно-коммуникационным системам, опасаясь серьезных нарушений в этих системах, а с другой стороны, признает необходимость свободы и открытости Интернет-пространства. В стратегии дается определение кибербезопасности. “Кибербезопасность –это защищенность от сбоев и неправильной эксплуатации информационно-телекоммуникационных систем. Сбои и неправильная эксплуатация может отрицательно повлиять на доступность и надежность информационно-телекоммуникационных систем, поставить под угрозу конфиденциальность и целостность информации, хранящейся в системах”.

Соединенное Королевство (2011): Подход Соединенного Королевства также направлен на развитие кибербезопасности. Цель: вывести Соединенное Королевство на первое место по инновациям, инвестициям и качеству сервисов в сфере информационно-телекоммуникационных технологий, и тем самым, в полной мере воспользоваться всеми преимуществами и достоинствами киберпространства. Необходимо исключить риски типа кибератак преступников, террористов и других государств с целью сделать киберпространство безопасным для граждан и экономики.

3. Стратегии кибербезопасности в странах, не входящих в Евросоюз

Ниже изложены краткие выдержки из стратегий трех стран, не входящих в Евросоюз. Помимо перечисленных, множество других стран также имеют опубликованные стратегии кибербезопасности, например: Индия, Австралия, Новая Зеландия, Колумбия, – и этими странами список далеко не исчерпывается. Тем не менее, список стран показывает, что проблема кибербезопасности признается важной во всем мире.

Соединенные Штаты Америки

США опубликовали Международную Стратегию для киберпространства в мае 2011 года[10]. Стратегия описывает ряд мероприятий, которые нужно провести по семи направлениям. В основе стратегии лежит модель сотрудничества между правительством, международными партнерами и частным сектором:

Экономика: продвижение международных стандартов и инновационных, открытых рынков.

Защита национальных сетей: повышение безопасности, надежности и отказоустойчивости. Правопорядок: расширение сотрудничества и правовых норм.

Военная отрасль: подготовка к современным вызовам безопасности.

Интернет-правительство: продвижение эффективных и всеохватывающих правительственных структур.

Международное развитие: построение безопасности, развитие международной компетенции и экономическое процветание.

Свобода в Интернете: поддержка основных свобод и неприкосновенности частной жизни.

Канада

Опубликованная в 2010[11] году стратегия кибербезопасности держится на трех “столпах”:

Защита правительственных систем.

Сотрудничество с целью защиты ключевых кибер-систем, находящихся за пределами федерального Правительства.

Обеспечение безопасности канадских граждан в онлайн-среде.

Первый “столп” подразумевает установление четких ролей и ответственности, усиление безопасности кибер-систем федерального уровня и повышение информированности правительства в области кибербезопасности.

Второй “столп” – это ряд партнерских проектов государственного уровня с привлечением частного сектора и секторов критических инфраструктур.

И, наконец, третий “столп” – это борьба с киберпреступностью и защита канадских граждан в онлайн-среде. Здесь также затрагивается проблема персональных данных.

Япония

Стратегию кибербезопасности Японии[12] (май 2010 года) также можно подразбить на несколько ключевых областей действия:

Усиление политик, направленных на борьбу с возможными массовыми кибератаками и учреждение органа, ответственного за предотвращение атак.

Введение политик, легко адаптирующихся к изменениям в сфере информационной безопасности.

Предпочтение активных политик информационной безопасности пассивным.

Основные мероприятия, описанные в стратегии Японии, включают в себя:

Управление IT-рисками для обеспечения безопасной жизни общества.

Внедрение политики, которая усилит государственную безопасность, улучшит управление кризисами в киберпространстве, и не будет противоречить политике использования информационно-коммуникационных систем, которая служит основой для социоэкономической деятельности.

Введение трехчастной политики, комплексно затрагивающей проблемы национальной безопасности, управление кризисами и защиту общества/личности. В особенности важна политика информационной безопасности общества/личности.

Введение политики информационной безопасности, которая не противоречила бы стратегии экономического роста.

Развитие международных альянсов.

4. Общие принципы

Как на европейском, так и на международном уровне согласованного определения кибербезопасности нет[13]. В каждой стране определение кибербезопасности и других ключевых терминов[14] может значительно различаться. Как следствие, различаются и подходы к составлению стратегий кибербезопасности. Отсутствие общего “языка” и подхода усложняет процесс международного сотрудничества, когда как важность сотрудничества признается всеми странами.

Как правило, в стратегии кибербезопасности затрагиваются следующие темы:

Построение правительственной модели, направленной на обеспечения кибербезопасности.

Определение подходящего механизма (в основном общественно-государственного партнерства), позволяющего частным и государственным заинтересованным сторонам обсуждать и утверждать политики, связанные с проблемой кибербезопасности.

Планирование и определение необходимых политик и регулирующих механизмов, четкое обозначение ролей, прав и ответственности для частного и государственного сектора (например, новая законодательная база для борьбы с киберпреступностью, обязательное информирование об инцидентах безопасности, базовые меры обеспечения безопасности и руководства к действию, новые нормы материально-технического обеспечения). К примеру, в стратегии Словакии обозначена необходимость создания законодательной базы для защиты киберпространства.[15]

Определение целей и способов развития государственных возможностей и необходимой законодательной базы для вступления в международную борьбу с киберпреступностью. В некоторых стратегиях киберпреступности уделяется особое внимание. Например, Голландия нацелена на расследование и уголовное преследование преступлений в киберпространстве. [16] Франция также придерживается этой точки зрения, страна желает усиливать существующее законодательство и развивать международное правовое сотрудничество. [17]

Определение ключевых информационных инфраструктур (critical information infrastructures – CIIs), в том числе основных активов, сервисов и взаимозависимостей.

Повышение готовности, уменьшение времени реакции на инциденты, разработка плана восстановления после сбоев и механизмов защиты для ключевых информационных инфраструктур (например, национальный план действий в особой обстановке, порядок поведения в киберпространстве, ситуационная осведомленность). В литовской стратегии утверждается, что “для обеспечения безопасности киберпространства необходимо организовать непрерывно функционирующую и надлежащим образом управляемую систему, контролирующую все стадии управления инцидентами, начиная от раннего предупреждения, предотвращения, обнаружения, устранения, и заканчивая расследованием инцидента.” [18] Кроме того, необходимо определить интегрированные организационные структуры, в обязанности которых входит разработка, внедрение и тестирование средств повышения готовности, планов восстановления после сбоев и механизмов защиты. Также возможна интеграция существующих структур, например, национальных/правительственных групп реагирования на чрезвычайные ситуации (CERTs).

Разработка системного и интегрированного подхода к государственному управлению рисками (например, доверенный обмен информацией и государственные реестры рисков).

Определение и обозначение целей информационных программ, призванных привить пользователям новые модели поведения и модели работы.

Доказательство необходимости новой программы образования, делающей упор на обучение IT-специалистов и профессионалов в области кибербезопасности. Необходимы также тренинги, улучшающие навыки пользователей. Например, в стратегии Соединенного Королевства ставится цель улучшить образовательные программы специалистов по информационной безопасности, чтобы построить надежный профессиональный фундамент для обеспечения кибербезопасности. [19]

Международное сотрудничество, как со странами - членами Евросоюза, так и со странами, не входящими в Евросоюз (например, принятие международных соглашений).

Проведение комплексного исследования и разработка программы развития, направленной на разрешение проблемы безопасности и отказоустойчивости как существующих, так и будущих систем и сервисов (например, интеллектуальные устройства).

5. Стратегия безопасности Интернета Евросоюза

В настоящий момент единой стратегии кибербезопасности для всего Евросоюза нет. Тем не менее, в программе работы Европейской комиссии на 2012 год [20] утверждается, что комиссия разработает Стратегию безопасности Интернета для Евросоюза. Разработку стратегии берет на себя главный директорат DG CONNECT (DG INFSO[21]). Цели проекта следующие:

Наравне с основными рисками и проблемами выявить экономические и геополитические возможности.

Сравнить между собой степень подготовленности и политическое внимание к проблеме безопасности Интернета в третьих странах.

Обозначить основные и важнейшие проблемы, которые требуют решения.

Оценить текущие и планируемые мероприятия, а также отметить те проблемные зоны, к которым Евросоюзу следует уделить больше внимания. [22]

Стратегия кибербезопасности и стратегия безопасности Интернета – это несколько разные вещи, хотя они имеют много общего, например, определение и предложение подходящей

правительственной модели, нацеленность на предотвращение и борьбу с инцидентами безопасности.

В целом же задача главного директората DG CONNECT – правильно разместить существующие и планируемые мероприятия в глобальном политическом контексте. Директорат также подготовит программу дальнейших действий, заглядывая вперед, чтобы предложить Евросоюзу комплексный, целостный и структурированный подход к проблеме безопасности Интернета. [23] Для реализации проекта компетенции одного только директората DG CONNECT будет недостаточно, именно поэтому вице-президент Европейской комиссии Нили Кроес (Neelie Kroes) подтвердила, что работа по проекту ведется в тесном сотрудничестве с комиссаром по внутренним делам Сесилией Мальмстрём (Cecilia Malmström) и Верховным Представителем по иностранным делам и политике безопасности Кэтрин Эштон (Catherine Ashton). [24]

Необходимость в предложении и достижении комплексного и скоординированного подхода подчеркивалась уже не один раз: об этом говорилось в документе ENISA 2011 года “Кибербезопасность: будущие вызовы и возможности”[25] , а также в докладе Палаты Лордов на совете по стратегии внутренней безопасности Евросоюза. [26]

6. Выводы и рекомендации

В среде, где постоянно появляются и эволюционируют кибер-угрозы, страны-члены Евросоюза при встрече с новыми, глобальными угрозами получат большую выгоду от гибких, оперативных стратегий кибербезопасности. Трансграничный характер угроз вынуждает страны вступать в тесное международное взаимодействие. Сотрудничество на пан-европейском уровне необходимо не только для эффективной подготовки к кибератакам, но и для своевременной реакции на них. Комплексная государственная стратегия кибербезопасности – первый шаг на этом пути.

Для стран-членов Евросоюза рекомендуется следующее:

В краткосрочном периоде:

Спроектировать, переоценить и поддерживать государственную стратегию кибербезопасности, а также мероприятия, проводимые в рамках стратегии.

Четко определить рамки действия, цели стратегии и само толкование термина “кибербезопасность”.

Убедиться, что предложения и заявления министерств, регулятивных органов и других государственных органов приняты во внимание и рассматриваются.

Учесть в стратегии интересы промышленности, научного сообщества и гражданских представителей.

Сотрудничать с другими странами, входящими в Евросоюз, а также с комиссией Евросоюза, чтобы гарантировать согласованный характер кибербезопасности.

Признать, что непрекращающееся развитие киберпространства и кибербезопасности отразится в постоянном редактировании и пересмотре стратегии.

Осознать, что предыдущий пункт подразумевает не только появление новых угроз и рисков, но и появление новых возможностей улучшения информационных систем для правительства, промышленности и общества.

Убедиться, что в стратегии принимается во внимание уже проделанная работа по повышению уровня безопасности национальных и пан-европейских информационных систем. Необходимо избегать дублирования мероприятий и сфокусироваться на новых проблемах.

Поддержать комиссию Евросоюза в деле создания Стратегии безопасности Интернета.

В долгосрочном периоде:

Договориться об общепринятом толковании термина “кибербезопасность” для того, чтобы в дальнейшем сформулировать общие цели для всего Евросоюза.

Убедиться, что стратегии кибербезопасности Евросоюза и его членов не противоречат целям международного сообщества, а поддерживают борьбу с проблемами кибербезопасности на глобальном уровне.

Для реализации стратегий кибербезопасности частный и государственный сектора должны работать в тесном сотрудничестве. Сотрудничество должно осуществляться посредством обмена информацией, передовыми практиками (например, в сфере управления инцидентами), а также учениями на государственном и пан-европейском уровне.

Для содействия комиссии и странам-членам Евросоюза в нелегкой миссии по созданию стратегии ENISA разрабатывает специальное руководство (Good Practices Guide). В руководстве будут содержаться передовые практики и рекомендации по проектированию, внедрению и поддержке государственной стратегии кибербезопасности. Руководство будет полезным инструментом и практическим советом для людей, ответственных или вовлеченных в проектирование стратегии. Руководство разрабатывается в содействии с частными и государственными заинтересованными сторонами со всей Европы. В разработке руководства также

принимают участие некоторые международные стороны, которые проводят среднесрочный анализ рекомендаций ENISA.

[1]Немецкая стратегия, стр. 1

[2]Например: COM/2005/0229 final “i2010 – A European Information Society for growth and deployment”; COM(2006) 251 “A Strategy for a Secure Information Society”; COM(2010) 245 final/2 “A Digital Agenda for Europe”; COM(2009) 149 on Critical Information Infrastructure Protection

[3]DIRECTIVE 2009/140/EC

[4]COM(2011) 163 final “Achievements and next steps: toward global cyber-security”

[5]Способность сети предоставлять и поддерживать приемлемый уровень сервиса во время отклонений от штатного режима работы, ‘Обзор стран-членов Евросоюза’ нормативные документы, связанные с надежностью работы телекоммуникационных сетей общего доступа, ENISA, 2008

[6]http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

[7]http://www.dhs.gov/files/publications/editorial_0329.shtm

[8]http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf

[9]Ссылки на стратегии кибербезопасности стран-членов Евросоюза можно найти в приложении

[10]http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[11]http://publications.gc.ca/site/eng/379746/publication.html

[12]http://www.nisc.go.jp/eng/

[13]H. Luiijf, K. Besseling, M. Spoelstra, P. de Graaf, Ten National Cyber Security Strategies: a comparison, CRITIS 2011 – 6th International Conference on Critical information infrastructures Security, September 2011.

[14]Определение киберпространства, киберпреступности и стратегии кибербезопасности также различается в разных странах.

[15]Стратегия Словакии, стр.10

[16]Голландская стратегия, стр.12

[17]Французская стратегия, стр. 8

[18]Стратегия Литвы, стр. 4

[19]Стратегия Соединенного Королевства, стр. 29

[20]COM(2011) 777 final VOL.1/2http://ec.europa.eu/atwork/programmes/docs/cwp2012_en.pdf

[21]С 1-го июля 2012 года DG INFSO переименовано в DG CONNECT

[22]COM(2011) 777 final VOL.2/2http://ec.europa.eu/atwork/programmes/docs/cwp2012_annex_en.pdf

[23]ROADMAP:Proposal on a European Strategy for Internet Securityhttp://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

[24]SPEECH/12/204http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/204

[25]http://www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities

[26]http://www.publications.parliament.uk/pa/ld201012/ldselect/ldeucom/149/149.pdf

Часть II

Статистические и справочные материалы

ИНТЕРНЕТ-БЕЗОПАСНОСТЬ*

Под компьютерной Интернет-безопасностью традиционно понимается:
защита от компьютерных вирусов;
защита от несанкционированного доступа к информации;
сохранение информации при сбоях;
защита от спама;
защита от мошенничества;
борьба с пиратством.

«Лаборатория Касперского» (www.kaspersky.ru) составила портрет типичного российского Интернет-пользователя на основе данных 14,6 млн россиян за 2011 г. Среднестатистический рунетчик пользуется операционной системой Windows XP (55%), а не более защищенной Windows 7. В среднем компьютер нашего соотечественника содержит 11 уязвимостей в установленном программном обеспечении (ПО). Три четверти пользователей посещали сайты, содержащие вредоносное ПО. Чаще всего на них вели ссылки с порносайтов (33% случаев), развлекательных сайтов (16%), ресурсов с пиратским ПО (14%), а также социальных сетей (10%). Большинство таких вредоносных хостингов зарегистрировано на территории России. У 56% пользователей хотя бы раз в год срабатывал веб-антивирус – это самый большой в мире показатель. Самой крупной мишенью для киберпреступников является браузер Internet Explorer – 17% срабатываний антивируса зарегистрировано в нем. Следом идут Mozilla Firefox – 14%, Google Chrome – 11%, Opera – 8%. 7% российских пользователей регулярно подвергаются фишинговым атакам – на одного пользователя в среднем приходится 10 фишинговых атак в год (фишинг — Интернет-мошенничество с целью получения доступа к логинам и паролям). Чаще всего это происходит на поддельных Интернет-сайтах, выдающих себя за «Google», «Яндекс», «Mail.ru», «Microsoft», «Одноклассники», «ВКонтакте», «Facebook». В целом в течение 2011 г. российские пользователи стали жертвами 939 млн сетевых атак (64 на одного пользователя в среднем). Велика киберугроза для подростков. Среднестатистический российский подросток пытается попасть на порносайты (76% от общего количества попыток), ресурсы, содержащие пиратское ПО (64%), порталы с азартными играми (38%). Специалисты «Лаборатории Касперского» считают, что угрозы безопасности сместились от кибервандализма к мошенническому ПО. Ранее угроза для компьютеров в основном исходила от вирусов и червей. Сегодня наиболее значительную угрозу представляет мошенничество с целью получения незаконных доходов. Для борьбы с вирусами сформирован рынок антивирусного ПО. В России популярны следующие компании и системы:

«Лаборатория Касперского»; «Доктор Веб»; «ESET NOD32»; «Panda Software»; «McAfee»; «Symantec»; «McAfee Antivirus»; «Computer Associates Antivirus»; «Trend Micro Titanium Antivirus»; «Shield Deluxe».

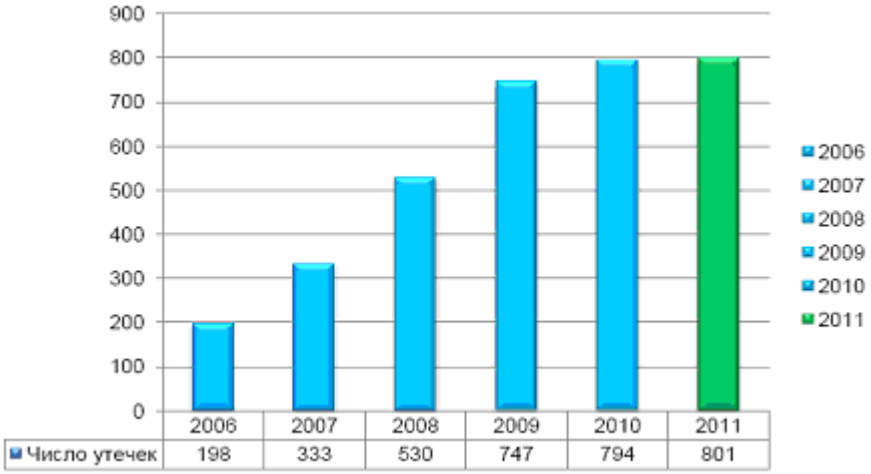
По прогнозам аналитиков фирмы «Canalys» (www.canalys.com), расходы на корпоративные программные средства компьютерной безопасности в 2012 г. вырастут в мире по сравнению с 2011 г. на 8,7% и достигнут 22,9 млрд долл. Небольшие компании будут постепенно отвоевывать долю рынка у мировых лидеров в области производства ПО, таких, например, как компания «Symantec». Одной из самых быстрорастущих компаний на российском рынке является «Лаборатория Касперского». Еще одна болевая точка Рунет – пиратство. Международный союз по защите интеллектуальной собственности (IIPA, www.iipa.com) опубликовал ежегодный доклад за 2011 г. о распространении пиратства в мире. Россия в этом докладе поднялась с десятого на четвертое место в мире по количеству скачиваний нелегального контента на торрент-ресурсах. Российские пользователи в течение

*Отчет «Интернет в России. Состояние, тенденции и перспективы развития в 2011 году»: извлечение // Опубликовано на официальном сайте Федерального агентства по печати и массовым коммуникациям *http://www.fapmc.ru/*

года произвели почти 31 млн загрузок нелегальных копий голливудских картин. IIPA фиксирует, что единственной сферой, демонстрирующей положительный тренд, остается офисное программное обеспечение, уровень пиратства в котором сократился с 87% в 2004 г. до 65% по итогам 2010-го. Тем не менее, в 2011 г. количество уголовных дел против пользователей нелегального контента в этой сфере сократилось до 63 (78 в прошлом году), а количество обвинительных приговоров – с 41 до 19. На одно широкополосное подключение к Интернет в России приходится в среднем $11,1, потраченных в год на легальную музыку в сети. Для сравнения, во Франции этот показатель составляет $58,8, в США – $82,6, в Великобритании – $97,5. Проблемой для индустрии остаются сервисы с бесплатным или дешевым нелицензированным контентом, в том числе, социальной сети «ВКонтакте» – крупнейшего дистрибутора контрафактной музыки в России и одного из крупнейших в мире.

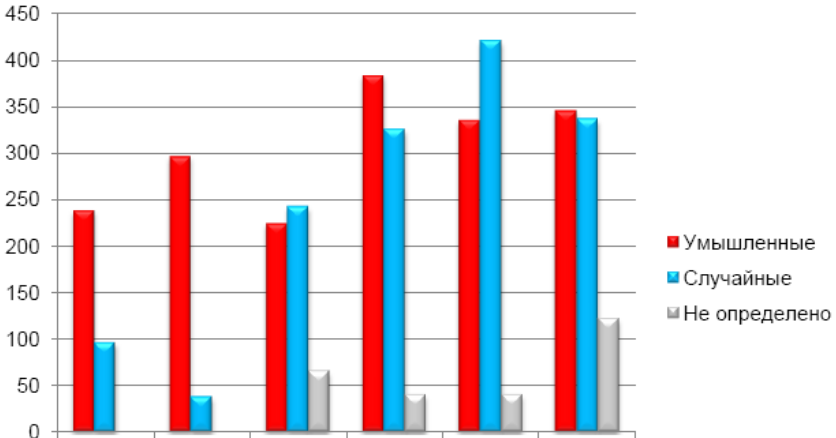
INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

ДИНАМИКА ЧИСЛА УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, 2006-2011 гг.*



	2006	2007	2008	2009	2010	2011
Число утечек	198	333	530	747	794	801

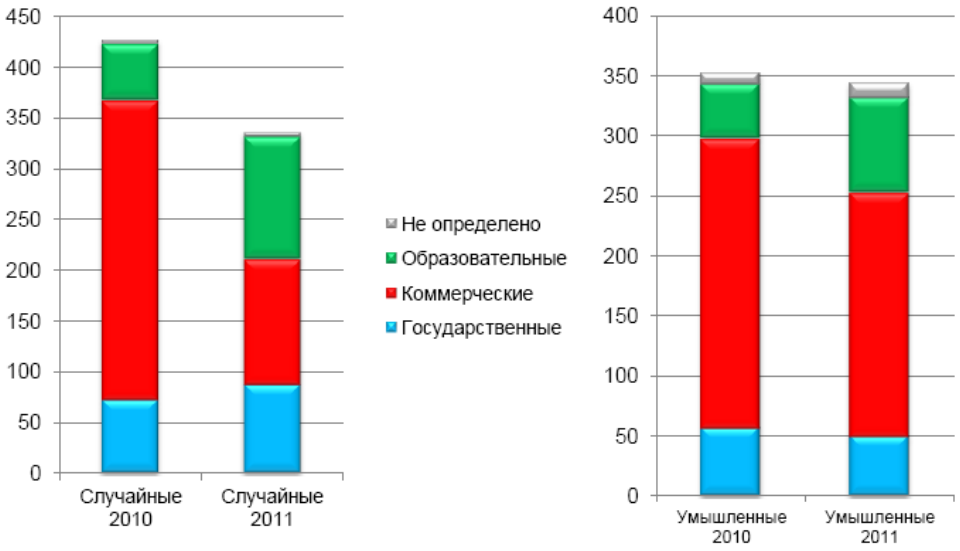
ДИНАМИКА СООТНОШЕНИЯ СЛУЧАЙНЫХ И УМЫШЛЕННЫХ УТЕЧЕК, 2006-2011 гг.



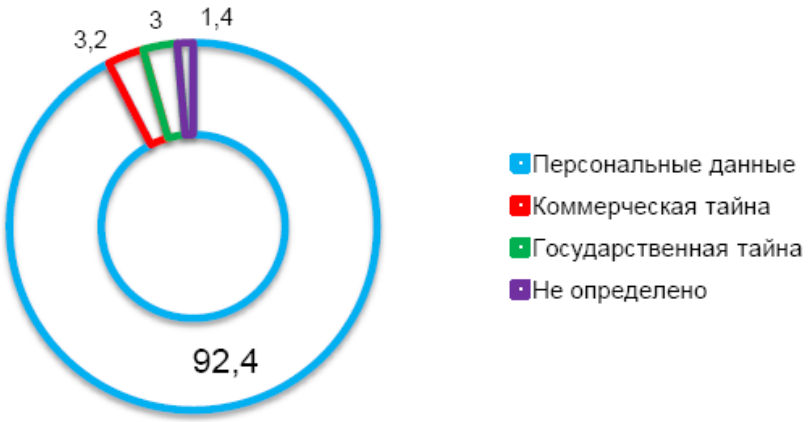
	2006	2007	2008	2009	2010	2011
Умышленные	237	295	223	382	334	344
Случайные	96	38	242	325	420	336
Не определено	0	0	65	40	40	121

*Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2011 г.: извлечение // Опубликовано на сайте Аналитического центра InfoWatch *http://www.infowatch.ru/*

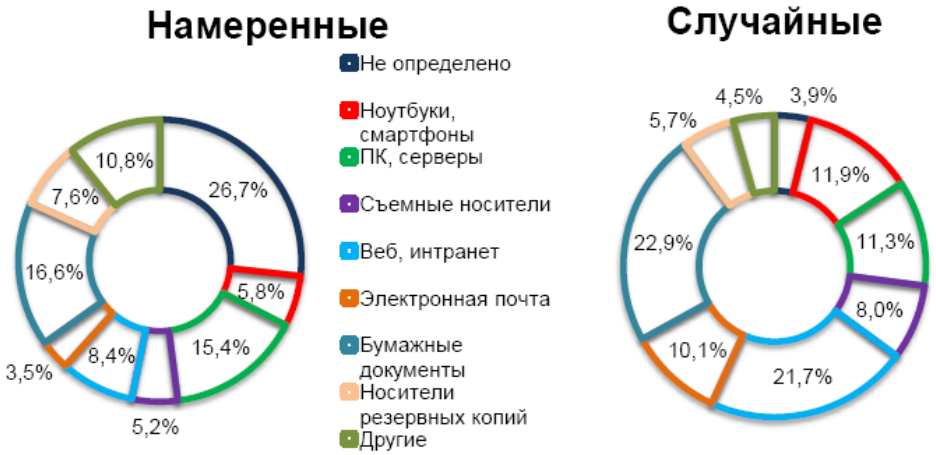
СООТНОШЕНИЕ СЛУЧАЙНЫХ И УМЫШЛЕННЫХ УТЕЧЕК ПО ТИПАМ ОРГАНИЗАЦИЙ, 2010-2011 гг.



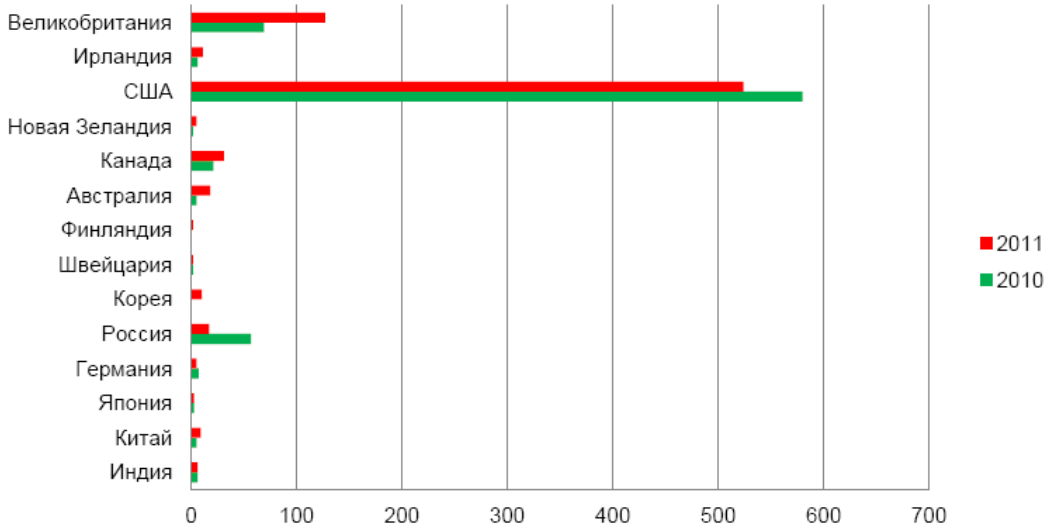
РАСПРЕДЕЛЕНИЕ УТЕЧЕК ПО ТИПАМ ДАННЫХ, 2011 г.



РАСПРЕДЕЛЕНИЕ СЛУЧАЙНЫХ И УМЫШЛЕННЫХ УТЕЧЕК ПО КАНАЛАМ, 2011 г.

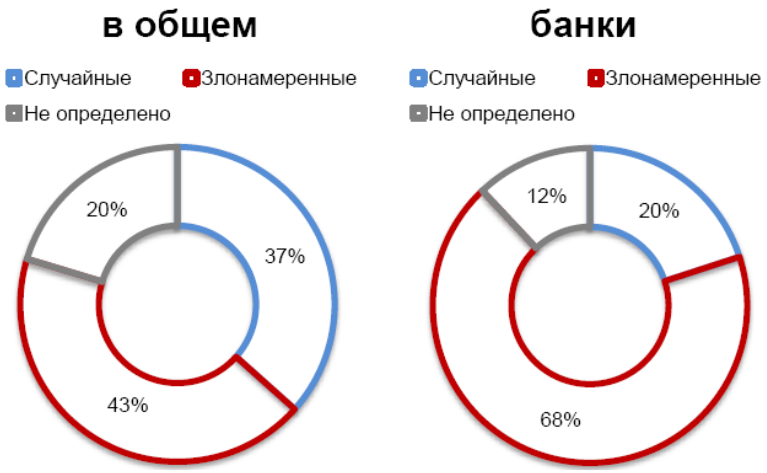


РАСПРЕДЕЛЕНИЕ ОБНАРОДОВАННЫХ УТЕЧЕК ПО СТРАНАМ, 2011 г., шт.



ДОЛЯ ФИНАНСОВЫХ И КРЕДИТНЫХ УЧРЕЖДЕНИЙ В ОБЩЕЙ СТАТИСТИКЕ УТЕЧЕК*

СООТНОШЕНИЕ СЛУЧАЙНЫХ И УМЫШЛЕННЫХ УТЕЧЕК



*Глобальное исследование утечек корпоративной информации и в банковском сегменте (финансовые и кредитные учреждения), 1 полугодие 2012 г.: извлечение // Опубликовано на сайте Аналитического центра InfoWatch *http://www.infowatch.ru/*

Часть III

Дополнительный список книг, авторефератов диссертаций, неопубликованных материалов парламентских мероприятий, публикаций в сборниках, журналах, газетах и интернет-ресурсах

2011 - 2013 гг.

Антонович П.И. О современном понимании термина «кибервойна» / П.И. Антонович // Вестник Академии военных наук. - 2011. - № 2. - С. 89-96

Антонович П.И. О сущности и содержании кибервойны / П.И. Антонович // Военная мысль. - 2011. - № 7. - С. 39-46

Артамонова Я.С. Методология выявления угроз в сфере информационной безопасности / Я.С. Артамонова // Социально-гуманитарные знания. - 2012. - № 1. - С. 111-126

Асланов Р.М. Зарубежный опыт правового регулирования обеспечения информационной безопасности / Р.М. Асланов // Политика и общество. - 2012. - № 2. - С. 45-48

Баулин А. Кибербитва за Родину / А. Баулин // Эксперт. - 2013. - № 4. - С. 46-49

Бедрицкий А.В. Международные договоренности по киберпространству: возможен ли консенсус? / А.В. Бедрицкий // Проблемы национальной стратегии. - 2012. - № 4. - С. 119-136

Быков В.М. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ / В.М. Быков, В.Н. Черкасов // Российский судья. - 2012. - № 5. - С. 14-19

Варфоломеев А.А. Кибердиверсия и кибертерроризм: пределы возможностей негосударственных субъектов на современном этапе / А.А. Варфоломеев // Военная мысль. - 2012. - № 12. - С. 3-11

Воронович Н.К. Интернет как угроза информационной безопасности России: автореф. дис. ... канд. социол. наук / Н.К. Воронович. - Краснодар, 2012. - 27 с.

Воронович Н.К. Информационный экстремизм в глобальной компьютерной сети Интернет / Н.К. Воронович // Общество и право. - 2012. - № 1. - С. 290-292

Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний / С.В. Воронцова // Российская юстиция. - 2011. - № 2. - С. 14-15

Государственные стратегии кибербезопасности / Европейское агентство по сетевой информационной безопасности (ENISA) // Опубликовано 4 сентября 2012 года на сайте информационного портала по безопасности SecurityLab.ru *http://www.securitylab.ru/*

Гребеньков А.А. Использование вредоносных программ для ЭВМ как средства ведения информационной войны: проблемы уголовно-правового противодействия / А.А. Гребеньков // Уголовное право: стратегия развития в XXI веке: материалы IX Междунар. науч.-практ. конф. (26-27 янв. 2012 г.) / Моск. гос. юрид. акад. - М., 2012. - С. 400-405

Гришин С.Е. Кибербезопасность и проблема повышения качества управления информацией / С.Е. Гришин, С.Г. Седышев // Вестник Саратовского государственного социально-экономического университета. - 2012. - № 1. - С. 202-206 (из фондов Научной электронной библиотеки *http://elibrary.ru*)

Джансараева Р.Е. Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ / Р.Е. Джансараева, К. Аратулы // Криминологический журнал Байкальского государственного университета экономики и права. - 2012. - № 3. - С. 95-99

Елин В.М. Интеграционные процессы в сфере борьбы с киберпреступностью на постсоветском пространстве / В.М. Елин // Интеграционное право: опыт Европы для постсоветского пространства: Междунар. науч.-практ. конф., г. Москва, 23 дек. 2010 г. / Моск. гос. юрид. акад. им. О.Е. Кутафина, Рос. новый ун-т. - М., 2011. - С. 57-66

Иванов М. Совет Федерации занялся цифровым суверенитетом / М. Иванов // Коммерсант. Daily. - 2012. - 6 нояб. - С. 3

Карамнов А.Ю. Проблемы квалификации в отношении преступлений, совершенных в глобальной сети Интернет / А.Ю. Карамнов // Правовые вопросы связи. - 2011. - № 1. - С. 22-23

Козориз Н.Л. Правовые основы обеспечения информационной безопасности военного управления / Н.Л. Козориз; М-во обороны Рос. Федерации, Воен. ун-т. - М., 2011. - 247 с.

Колесников А. Информационные технологии в РФ: сложности и перспективы / А. Колесников // Индекс безопасности. - 2013. - № 1. - С. 17-22 (из фондов Научной электронной библиотеки *http://elibrary.ru*)

Коробов И. Использование сети Интернет террористическими и экстремистскими организациями / И. Коробов // Зарубежное военное обозрение. - 2012. - № 6. - С. 23-26

Косовец А.А. Терроризм как объект противодействия в системе обеспечения информационной безопасности: международные и организационно-правовые аспекты / А.А. Косовец // Вестник Академии экономической безопасности МВД России. - 2011. - № 3. - С. 71-76

Крикунов А. Киберпространство ведущих государств в контексте современных вызовов и угроз / А. Крикунов // Морской сборник. - 2011. - № 11. - С. 32-37

Кузнецов П.У. Структура и содержание модели закона об информационной безопасности / П.У. Кузнецов // Вестник УРФО. Безопасность в информационной сфере. - 2012. - № 1. - С. 4-9

Кухаркин А. Киберугрозы и защиты информации / А. Кухаркин // Обозреватель - Observer. - 2012. - № 10. - С. 94-103

Мединн А. Использование киберпространства террористическими и экстремистскими организациями / А. Мединн, С. Маринин // Зарубежное военное обозрение. -2012. - № 10. - С. 3-8

Молодчая Е.Н. Политика противодействия кибертерроризму в современной России: политологический аспект: автореф. дис. ... канд. полит. наук / Е.Н. Молодчая. - М., 2011. - 30 с.

Нормативно-правовая база и методы противодействия Интернет-угрозам: материалы «круглого стола» / Комис. Совета Федерации по информ. политике. - М., 2011

Обеспечение безопасности в информационном обществе: материалы «круглого стола» / Ком. Совета Федерации по науке, образованию, культуре и информ. политике. - М., 2011

Овчинников С.А. О создании системы контроля обеспечения безопасности критически важных информационных сегментов органов государственной власти региона / С.А. Овчинников // Информационная безопасность регионов. - 2012. - № 1. - С. 8-12 (из фондов Научной электронной библиотеки *http://elibrary.ru*)

Паршин С.А. Кибервойны. Реальная угроза национальной безопасности? / С.А. Паршин, Ю.Е. Горбачев, Ю.А. Кожанов; Ин-т проблем междунар. безопасности РАН. - М., 2011. - 93 с.

Паршин С.А. Современные американские подходы к проблеме кибертерроризма / С.А. Паршин // Вестник Московского университета. Серия 25, Международные отношения и мировая политика. - 2011. - № 3. - С. 81-105

Пиджаков А.Ю. Противодействие кибертерроризму в зарубежных странах и проблемы его организации и правового регулирования в Российской Федерации / А.Ю. Пиджаков, Р.А. Шахбазов // Мир юридической науки. - 2012. - № 9. - С. 56-63

Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки / А.А. Протасевич, Л.П. Зверянская // Криминологический журнал Байкальского государственного университета экономики и права. - 2011. - № 3. - С. 28-33

Рассолов И.М. Административно-правовые проблемы обеспечения кибербезопасности / И.М. Рассолов // Государственный аудит. Право. Экономика. - 2012. - № 4. - С 166-173

Роговский Е.А. Политика США по обеспечению безопасности киберпространства / Е.А. Роговский // США. Канада: экономика, политика, культура. - 2012. - № 6. - С. 3-22

Сало И.А. Преступные действия с компьютерной информацией ограниченного доступа: автореф. дис. ... канд. юрид. наук / И.А. Сало. - М., 2011. - 24 с.

Смирнов А.А. Система борьбы с киберпреступностью в Европейском союзе / А.А. Смирнов // Библиотека криминалиста. - 2012. - № 2. - С. 262-274

Стельмах А.П. Обеспечение кибернетической безопасности Российской Федерации (основы общей киберологии) / А.П. Стельмах, А.В. Тонконогов. - М., 2012. - 101 с.

Степанова О.А. Перспективы международно-правового взаимодействия правоохранительных органов по противодействию кибертерроризму / О.А. Степанова // Актуальные проблемы современного международного права: материалы ежегод. межвуз. науч.-практ. конф., 9-10 апр. 2010 г./ Рос. ун-т дружбы народов; [отв. ред.: А. Х. Абашидзе и др.]. - М., 2011. - Ч. 2. - С. 295-299

Тонконогов А.В. Обеспечение кибернетической безопасности России в современных геополитических условиях / А.В. Тонконогов // Закон и право. - 2011. - № 10. - С. 5-6

Халиуллин А.И. Компьютерные преступления в уголовном законодательстве стран - участниц Содружества Независимых Государств / А.И. Халиуллин // Вестник Российской правовой академии. - 2012. - № 1. - С. 53-56

Чекунов И.Г. Киберпреступность: понятие и классификация / И.Г. Чекунов // Российский следователь. - 2012. - № 2. - С. 37-44

Чекунов И.Г. Понятие и типология киберпреступности / И.Г. Чекунов // Вестник Академии права и управления. - 2012. - № 26. - С. 68-73

Чирков П.А. Об объекте преступлений в сфере компьютерной информации в Российском уголовном праве / П.А. Чирков // Правовые вопросы связи. - 2012. - № 1. - С. 21-23

Швед Н.А. Уголовно-правовое регулирование ответственности за несанкционированный доступ к компьютерной информации за рубежом / Н.А. Швед // Правовые вопросы связи. - 2011. - № 1. - С. 38-40