УДК 338.24

ISSN 1812-5220

Новый вид рисков — риски киберпространства

Ю. И. Соколов,
ФГУ ВНИИ ГОЧС (ФЦ) МЧС России, 6 Центр,
г. Москва

Аннотация

В статье рассматриваются вопросы риска использования киберпространства при автоматизации управления промышленными объектами, критически важными объектами и в работе органов управления, а также обеспечения кибербезопасности.

Ключевые слова: Интернет, киберпространство, автоматизированные системы управления технологическим процессом, информационно-коммуникационные технологии, ключевые системы информационной инфраструктуры, компьютерные вирусы, хакер, киберугрозы, кибератаки, кибервойна, кибербезопасность.

Содержание

1. Интернет — колыбель киберпространства

Киберпространство обязано своим появлением Интернету. Интернет явился концентрированным отражением общих тенденций информационной революции конца XX — начала XXI века, который интегрирует не только коммуникационные и технологические ресурсы, но и материальные, финансовые, интеллектуальные, гуманитарные, политические и прочие ресурсы, формирует и диверсифицирует процессы социальной регуляции.

Компьютеризацией пронизаны все сферы множественных коммуникаций и средств обеспечения как и внутри страны, так и между странами, государствами. Вся инфраструктура городов и стран сейчас зависима от компьютеров. Интернет, как паутина, охватил все страны и континенты. Это как некий мозг с нервной системой. Цифровые технологии стали кровеносной и нервной системой человеческих коммуникаций и взаимодействий [1].

Интернет соединяет все компьютеры, ноутбуки, серверы, планшеты и смартфоны в одну большую машину, которая стала самым надежным механизмом из всех, что человек придумал. За последнее десятилетие Интернет стал неотъемлемой частью каждой из сторон нашей жизни, и его значимость продолжает возрастать. В настоящий момент более 44% населения мира являются пользователями Интернета.

Современная архитектура Интернета позволяет на основе интернет-инфраструктуры создать виртуальное интернет-поле, границы которого не зависят от национальных границ.

Появление киберпространства способствовало формированию глобального информационного пространства, становлению «сетевого общества», основой функционирования которого становятся генерирование, обработка, передача и обновление информационного социального поля. Киберпространство включается в социальную среду и является одним из важнейших факторов, способствующих глобализации, становится инфраструктурным фундаментом новых областей жизнедеятельности человечества.

Интернет становится все более значимым фактором изменений социоэкономического характера, демонстрируя технико-технологическую, экономическую и экспоненциально возрастающую социальную значимость как собственно в Сети, так и в реальной жизни и в нашей стране.

Сказать, что в нашей стране возможности, предоставляемые Интернетом, используются чрезвычайно широко, значит не сказать ничего. Экономика страны и качество жизни граждан находятся в зависимости от работоспособности национального сегмента Всемирной сети.

По данным последнего исследования «*Развитие Интернета в регионах России. Весна 2016*», аудитория Интернета в России на осень 2015 г. составляет 78 млн человек — столько россиян пользуются Интернетом хотя бы раз в месяц. А 63 млн человек выходят в Сеть ежедневно [2].

Проникновение Интернета в России немного меньше, чем в среднем по Европе, и существенно выше, чем в среднем в мире.

Количество интернет-пользователей в России к 2016 г. достигнет 100 млн. По данным министра связи и массовых коммуникаций РФ Н. Никифорова, увеличение доступа населения к Интернету на 10% дает примерно 1,5% экономического роста страны.

По данным Росстата, Интернет используют в своей работе 87% организаций. Большая часть информационного обмена как внутри коммерческих компаний, так и между ними осуществляется в электронной форме.

По тем же данным, 93% органов власти и муниципалитетов используют Интернет «для осуществления управленческих функций и предоставления государственных услуг».

В России работают 24 тыс. только официально зарегистрированных Роскомнадзором электронных средств массовой информации (26% от общего числа СМИ), число незарегистрированных как СМИ информационных сайтов составляет сотни тысяч.

В 2013 г. через Интернет продано 23 млн (20% от общего числа) железнодорожных билетов, а доля продаж электронных авиабилетов составила 97%.

Даже эти цифры подтверждают, что при потере работоспособности российского сегмента Интернета страна вернется в глубокое технологическое прошлое.

Глобальная информатизация в настоящее время активно управляет существованием и жизнедеятельностью государств мирового сообщества, информационные технологии применяются при решении задач обеспечения национальной, военной, экономической безопасности и др. Вместе с тем одним из фундаментальных последствий глобальной информатизации государственных и военных структур стало возникновение принципиально новой среды противоборства конкурирующих государств — киберпространства, которое не является географическим в общепринятом смысле этого слова, но тем не менее в полной мере является международным.

Развитие Интернета, открывшего для человечества невиданные ранее возможности в сфере информации и коммуникации, создании киберпространства, сопровождается также целым рядом невиданных раннее рисков:

- проявление киберпреступности против личности, государства, общества;
- сращивание национальной и зарубежной преступности в транснациональные преступные синдикаты;
- информационный вандализм и хакерство;
- информационный терроризм на внутригосударственном и международном уровнях;
- информационные войны на внутригосударственном и международном уровнях, которые способны вызвать взрывы на химических заводах и токсичные облака над мегаполисами, пожары на нефтехранилищах и трубопроводах, транспорт-

ный коллапс на дорогах и в аэропортах, а нация оказывается буквально парализована без электричества, управления, защиты и информации о том, что происходит.

Все это позволяет злоумышленникам совершать с помощью Интернета негативные деяния как против элементов Интернета, так и против иных субъектов Интернета, а также наносить прямой ущерб любым юридическим субъектам, и даже их критически важной инфраструктуре, если она подключена к Интернету.

В своем докладе 2013 г. об экономических последствиях киберпреступности компания McAfee привела оценку, что вероятные ежегодные потери глобальной экономики от киберпреступности составляют более 455 млрд долл. [https://digital.report/zashhita-ict-infrastrukturyi/].

Ущерб экономике Российской Федерации от действий киберпреступных групп в 2015 г. составил 203,3 млрд руб., или 0,25% от валового внутреннего продукта страны. Такие выводы содержатся в исследовании «*Киберпреступность в России и ее влияние на экономику страны*», подготовленном экспертами Group-IB, Фонда развития интернет-инициатив (ФРИИ) и Microsoft [https://servernews.ru/931430].

2. Киберпространство

Термин «киберпространство» — популярный термин для обозначения воспринимаемого пользователем «виртуального» пространства, содержащегося в памяти компьютера и изображенного графически. В середине 1990-х гг. этот термин приобрел широкое распространение в связи с развитием Интернета и Всемирной компьютерной сети (www).

Киберпространство представляет собой уникальную среду, не расположенную в географическом пространстве, но доступную каждому в любой точке мира посредством доступа в Интернет [1].

Общегосударственное определение киберпространства впервые прозвучало в докладе исследовательской службы конгресса США в 2001 г., где киберпространство определено как «всеохватывающее множество связей между людьми, созданное на основе компьютеров и телекоммуникаций вне зависимости от физической географии».

Термин «киберпространство» помогает осознать Интернет как новую форму пространства, не отвечающую материальным характеристикам, но позволяющую осуществлять в ней либо с ее помощью различные действия, которые могут иметь реальные последствия. Киберпространство является неотъемлемой частью современного мироустройства.

Киберпространство как противоположность естественному физическому пространству содержит информационный эквивалент вещей. Одна из главных составляющих киберпространства — это передвижение информации, которое осуществляется посредством программирования и цифровой коммуникации. Таким образом, определение термина «киберпространство» должно соотноситься с совокупностью множества процессов, которые осуществляются с использованием цифровых сетей: электронной перепиской, финансовыми операциями, разработкой и использованием компьютерных программ и созданием виртуальной реальности.

В начале 2014 г. Советом Федерации для публичного обсуждения был предложен проект концепции стратегии кибербезопасности Российской Федерации, которая должна была определить направления усилий государства в отношении новых угроз, возникающих в современном информационном мире.

Киберпространство в проекте концепции определяется следующим образом: «*Киберпространство — сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)*».

Данное определение во многом перекликается с позицией Международного стандарта ИСО/МЭК 27032:2012 «*Руководящие указания по кибербезопасности*». Киберпространство — это сложная среда, не существующая ни в какой физической форме, возникающая в результате взаимодействия людей, программного обеспечения, интернет-сервисов посредством технологических устройств и сетевых связей.

Важной особенностью киберпространства является его глобальность, обеспечивающая возможность информационного взаимодействия людей и объектов, располагающихся на территории различ-

ных государств. Глобальность киберпространства достигается посредством соединения национальных электронных сред в единую электронную среду сбора, передачи, хранения и обработки информации на основе единой системы цифровой адресации субъектов и объектов киберпространства.

3. Киберугрозы промышленным объектам

Киберпространство не замыкается в самом себе и повсеместно стыкуется с реальными объектами на программном уровне. Так, управление технологическими процессами, процессами производства материальных благ, системами безопасности все шире передается компьютерам и компьютерным программам, и защита автоматизированных систем управления технологическими процессами (АСУ ТП) все больше и больше выходит на передний край. Ведь АСУ ТП — это область, где виртуальный мир соприкасается с миром физическим.

На промышленных объектах АСУ ТП являются ключевыми системами информационной инфраструктуры. От корректной и стабильной работы этих систем зависит безопасность всего объекта. Большинство АСУ ТП, которые в настоящее время работают в промышленности, созданы без учета возможности кибератак.

Системы АСУ ТП в настоящее время применяются практически в каждой отрасли: начиная с транспортной (скоростные поезда «Сапсан», метрополитен), заканчивая атомными и гидроэлектростанциями, сетями распределения электроэнергии и водоснабжения.

Более 40% подключенных к Интернету АСУ ТП, применяющихся на предприятиях в энергогенерирующей, нефтеперерабатывающей и других отраслях, уязвимы для хакерских атак, в результате чего целые заводы могут быть выведены из строя, говорится в исследовании российской компании Positive Technologies [http://digit.ru/technology/20121107/396404269.html].

Последствия успешной хакерской атаки на любую из таких систем могут оказаться катастрофическими. Компания Positive Technologies является одним из мировых лидеров в области комплексной защиты крупных информационных систем от современных киберугроз.

Специалисты отмечают рост числа именно подключенных к Сети систем (еще несколько лет назад такие примеры были редкостью и АСУ ТП в основном работали автономно).

США и Европа лидируют по числу доступных из Интернета систем АСУ ТП, при этом 54% доступных извне систем в Старом Свете и 39% в США уязвимы и могут быть взломаны. На третьей позиции — Азия (32%). В России процент подключенных к Интернету АСУ ТП заметно ниже, однако страна входит в первую двадцатку государств с наибольшим количеством подобных сетевых ресурсов.

В настоящий момент 35% всех представленных уязвимостей АСУ ТП имеют эксплойты (готовые средства для использования уязвимости), которые свободно распространяются в виде отдельных утилит, входят в состав программных пакетов для проведения тестов на проникновение либо описаны в уведомлениях об уязвимости, отмечают исследователи.

Исследование охватило период с 2005 г. до 1 октября 2012 г. В период с 2005 по 2010 г. было обнаружено всего 9 уязвимостей в системах АСУ ТП. Однако после появления червя Stuxnet в 2010 г., который атаковал ряд ядерных объектов Ирана, за 2011 г. было найдено уже 64 уязвимости.

За первые восемь месяцев 2012 г. появились сообщения о 98 новых уязвимостях: это больше, чем за все предыдущие годы. При этом около 65% уязвимостей относятся к высокой и критической степени риска.

Исследования «Лаборатории Касперского», опубликованные в 2016 г., показали, что 92% подключенных к Интернету АСУ ТП уязвимы для киберугроз [https://www.pcweek.ru/security/news-company/detail.php?ID=186782].

Как выяснила «Лаборатория Касперского», большое количество автоматизированных систем управления (АСУ), использующихся на критически важных инфраструктурных и промышленных объектах, не только доступны из Интернета, но также имеют уязвимости в программном обеспечении, что подвергает их риску стать целью кибератаки. Кибератаки против критически важной гражданской инфраструктуры могут оставить тысячи человек без воды, еды и электричества, а диверсии против атомных электростанций и дамб — технически

они тоже возможны — могут привести к огромным жертвам.

В общей сложности эксперты компании обнаружили в 170 странах мира более 188 тыс. узлов, на которых размещено 220 тыс. разных промышленных систем, содержащих компоненты АСУ. Свыше 13 тыс. обнаруженных узлов принадлежат крупным компаниям, работающим в энергетике, нефтегазовой и химической отраслях, промышленном секторе, в сфере транспорта и автомобилестроения, в производстве продуктов питания, а также в области финансов и здравоохранения.

При развитии информационно-коммуникационных технологий в Российской Федерации широко применяются зарубежные аппаратно-программные средства. Очевидна возможность наличия в таких средствах программных или программно-аппаратных закладок, а также не декларированных возможностей. В большинстве зарубежных «защищенных микросхем» для коммерческого применения, в том числе предназначенных для защиты информации и продаваемых за пределы стран-изготовителей, предусмотрен «полицейский» режим, позволяющий получить доступ к ключевой информации и защищаемым данным, записанным в микросхемах.

В настоящий момент сложилась критическая ситуация, при которой на каждом из участков инфокоммуникационной инфраструктуры (чипы, схемотехника, электронные компоненты, транспорт и передача данных, системы управления, программное обеспечение от библиотек до отдельных продуктов и т.п.) с высокой долей вероятности используются зарубежные решения с неизвестной начинкой. Даже после проведения специальных мероприятий по проверке и анализу потенциально опасных свойств используемых решений нет оснований полагать, что данные свойства гарантированно не смогут проявиться при определенном наборе условий в дальнейшем [http://www.connect.ru/article.asp?id=10936].

Сегодня сложилась ситуация, когда на этапе ОКР по созданию продукта, гарантирующего соблюдение требований обеспечения кибербезопасности, невозможно получить результат, взаимодействуя только с российскими предприятиями.

Еще один пример похожей проблемы — зависимость от современных информационно-коммуникационных технологий (ИКТ). С одной стороны, государства продолжают массово закупать необходимые для развития их экономик современные технологии у относительно узкого круга поставщиков, что делает их уязвимыми перед решениями этих поставщиков (например, перед введением односторонних ограничений на поставки оборудования). Другой стороной этой же проблемы часто является невозможность проверить безопасность этого оборудования на всех уровнях — как программном, так и техническом. В итоге большинство стран мира оказываются заложниками узкого круга компаний и тех специальных структур, с которыми эти компании сотрудничают.

Именно поэтому и Совет безопасности, и руководство страны уделяют значительное внимание вопросам безопасности АСУ ТП критически важных объектов. В развитие принятых Советом безопасности решений 15 января 2013 г. Президентом Российской Федерации был подписан указ о создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Данным указом определен федеральный орган, на который возложены полномочия по созданию такой системы, — Федеральная служба безопасности.

4. Киберугрозы для критически важных объектов и ключевых систем информационной инфраструктуры

Критически важным признается объект (КВО), оказывающий существенное влияние на национальную безопасность Российской Федерации, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны либо для жизнедеятельности населения, проживающего на соответствующей территории. На территории Российской Федерации функционирует около 4,5 тыс. КВО [4, 5].

Основным признаком принадлежности объекта к критически важным является наличие на нем экологически опасного или социально значимого производства либо технологического процесса, нарушение штатного режима которого приводит к чрезвычайной ситуации определенного уровня и масштаба, или наличие на объекте информационно-телеком-

муникационной системы (ее элемента), которая осуществляет функции управления чувствительными (важными) для Российской Федерации процессами и нарушение функционирования которой приводит к негативным для страны последствиям.

Критически важными являются объекты, прекращение или нарушение функционирования которых может привести к тяжелым последствиям для региона или государства в целом, в том числе и к человеческим жертвам.

Перечни видов критически важных объектов и критически важных систем составляются специально создаваемой группой экспертов, состав которой утверждается соответствующим руководителем федерального органа исполнительной власти (организации).

Критичность объекта и соответственно его инфраструктуры во всем мире определяется на государственном уровне, критические для существования и функционирования государств предприятия и отрасли фиксируются в специальных перечнях. Естественно, государствообразующими являются самые различные секторы и отрасли — от финансовой и банковской системы до систем управления водо- и энергоснабжением.

Если говорить об отраслях, наиболее часто относимых к критической инфраструктуре и связанных не только с физической, но и с кибербезопасностью, то на основании усредненного мирового опыта можно составить следующий перечень, в определенной степени совпадающий у большинства государств [http://www.pircenter.org/media/content/files/13/14683392340.pdf]:

- электроэнергетика (атомная энергетика часто выделяется отдельно);
- управление природными ресурсами (в частности, нефтегазовый сектор);
- управление водными ресурсами (включая водоочистку и управление сточными водами);
- транспорт;
- пищевая промышленность;
- здравоохранение;
- телекоммуникации;
- финансовая и банковская системы;
- органы государственной власти.

Сюда же следует отнести и объекты жизнеобеспечения. *Объекты жизнеобеспечения* — объекты, обеспечивающие жизнедеятельность населения. К таковым относятся объекты водоснабжения (насосно-фильтровальные станции, станции очистки сточных вод, плотины, гидроузлы, водозаборы, водохранилища, дамбы, водосбросные, водоспускные и водовыпускные сооружения и т. п.), теплоснабжения (ТЭЦ, крупные городские котельные, работающие под давлением более 0,07 МПа или при температуре нагрева воды более 115 °С), энергоснабжения (ГРЭС, трансформаторные подстанции мощностью свыше 110 кВт).

Следствиями нарушения функционирования критически важного объекта могут быть:

- гибель или физическое травмирование людей;
- нарушение систем обеспечения жизнедеятельности городов и населенных пунктов;
- нарушение социальной стабильности в стране, регионе, субъекте Федерации, области, районе;
- авария или катастрофа, разрушение или заражение среды обитания в национальном масштабе;
- нанесение крупного экономического (финансового) ущерба государству, государственным и частным предприятиям и организациям, физическим лицам, нарушение стабильности финансовой и банковской системы страны, остановки непрерывных производств;
- крупномасштабное уничтожение национальных ресурсов (природных, сельскохозяйственных, продовольственных, производственных, информационных);
- нарушение системы государственного управления на федеральном, региональном и территориальном уровне;
- нанесение крупного внешнеполитического ущерба стране;
- причинение значительного ущерба в сфере обороны и безопасности страны.

Эффект от поражения программными средствами объектов критической инфраструктуры уже не исчерпывается похищением данных, а переходит в плоскость нанесения физического ущерба работе промышленных и логистических объектов вплоть до их полного разрушения.

Символом беспрецедентной опасности кибернетических атак стал компьютерный червь Stuxnet, который в 2009—2010 гг. поразил информационные системы иранского комбината по обогащению урана.

Дальнейшее развитие подобных средств программного воздействия уже позволяет применять их для осуществления диверсий на электростанциях, в том числе для разрушения энергогенерирующих турбин атомных электростанций и тому подобных составляющих критической атомной инфраструктуры. Подобные последствия выходят за рамки национальных границ государств, чья инфраструктура подвергается атакам, и представляют непосредственную угрозу международной безопасности наравне с международным терроризмом, трансграничной преступностью, а в перспективе и использованием оружия массового уничтожения.

Разработка и применение подобных программных инструментов осуществляется анонимно, в силу того, что существующие технические возможности не позволяют достоверно и однозначно идентифицировать конечный источник атаки и непосредственного ее автора. Кроме того, даже при наличии технической возможности определить, откуда осуществляется атака, не существует каких бы то ни было юридических и международно-правовых механизмов, позволяющих отнести ответственность за осуществление такой деятельности на конкретное лицо и тем более субъект международного права.

В таблице перечислены отрасли экономики России, наиболее уязвимые с точки зрения компьютерной безопасности.

Ключевая система информационной инфраструктуры (КСИИ) — это информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), либо информационное обеспечение управления таким объектом (процессом), либо официальное информирование граждан [5]. В результате деструктивных информационных воздействий на КСИИ может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

Системы, относящиеся к КСИИ

Информационные (информационно-телекоммуникационные) системы относятся к ключевым в зависимости от их назначения в соответствии с перечнем критически важных сегментов информационной инфраструктуры. В свою очередь, критически важными сегментами информационной и телекоммуникационной инфраструктуры России признаются сегменты, образуемые системами, нарушение штатного режима функционирования которых может нарушить функции управления чувствительными для Российской Федерации процессами, в том числе:

- системами органов государственной власти и органов местного самоуправления;
- системами органов управления правоохранительных структур;
- системами финансово-кредитной и банковской деятельности;

Отрасли экономики России, наиболее уязвимые с точки зрения компьютерной безопасности, % *Таблица*
[http://cs.groteck.ru/IB_6_2014/files/ib_6_2014.pdf]

Отрасль	Очень уязвимы	В какой-то степени уязвимы	Неуязвимы	Абсолютно неуязвимы	Всего
Аэрокосмическая и оборонная	22	30	33	15	51
Химическая	15	37	40	8	52
Финансы	32	36	24	8	68
Правительство и госорганы	21	39	29	10	61
Медицина/здравоохранение/фармацевтика	17	45	32	6	62
Нефтегазовая	16	39	36	9	55
Энергетика	15	39	37	8	54
Телекоммуникации/IT	27	42	26	6	68
Туризм	25	30	29	6	65

• системами предупреждения и ликвидации кризисных и чрезвычайных ситуаций;

• географическими и навигационными системами;

• программно-техническими комплексами центров управления взаимоувязанной сети связи России;

• сетями связи общего пользования на участках, не имеющих резервных или альтернативных видов связи;

• системами специального назначения;

• спутниковыми системами, используемыми для обеспечения органов управления и в специальных целях;

• системами управления добычей и транспортировкой нефти, нефтепродуктов и газа;

• системами управления потенциально опасными объектами;

• системами управления транспортом (наземным, воздушным, морским);

• системами управления водоснабжением;

• системами управления энергоснабжением.

Таким образом, в категорию КСИИ попадают не только многочисленные АСУ ТП, но и системы государственного управления, телевидения, банковской отрасли.

5. Крупные атаки хакеров в 2000—2015 годах

В апреле 2000 г. хакеры получили контроль над газовыми потоками «Газпрома» [https://lenta.ru/internet/2000/04/27/gasprom].

25 января 2003 г. в Республике Корея в результате действий хакеров произошел общенациональный сбой в Интернете, в течение нескольких часов вся страна была лишена доступа в мировую сеть. Впервые действия кибертеррористов отразились на деятельности компаний в общенациональном масштабе. Помимо Южной Кореи пострадали интернет-пользователи множества других стран, включая Россию, по всему миру были поражены по меньшей мере 22 тыс. серверов [http://tass.ru/info/1408961].

В апреле 2009 г. киберпреступники проникли в компьютерную систему Пентагона и похитили информацию о новом многоцелевом истребителе пятого поколения Joint Strike Fighter.

7 июля 2009 г. хакеры вывели из строя практически все важнейшие интернет-порталы в Южной Корее, включая сайты президента, парламента и министерства обороны.

В сентябре 2010 г. вирус Stuxnet поразил компьютеры сотрудников АЭС в Бушере (Иран) и создал проблемы в функционировании центрифуг комплекса по обогащению урана в Натанзе. По мнению экспертов, Stuxnet стал первым вирусом, который был использован как кибероружие.

23 апреля 2013 г. группа хакеров взломала аккаунт информагентства AP в сервисе микроблогов Twitter и разместила ложное сообщение о взрывах в американском Белом доме и ранении президента Барака Обамы.

В мае 2013 г. газета The Washington Post, ссылаясь на конфиденциальный доклад, направленный руководству Пентагона, сообщила, что в распоряжение китайских хакеров попали секретные военные документы США, включая чертежи и описания военных самолетов и кораблей, а также систем противоракетной обороны.

27 ноября 2013 г. и 15 декабря 2014 г. хакеры похитили персональные данные (номера телефонов, электронные и почтовые адреса, номера и PIN-коды кредитных и дебетовых карт) 110 млн клиентов компании Target, владеющей третьей по величине торговой сетью США. В результате американские финансовые институты понесли убытки в размере более 200 млн долл.

16 февраля 2015 г. в результате хакерской операции Carbanak киберпреступники украли около миллиарда долларов из 100 финансовых организаций по всему миру. Об этом говорится в сообщении компании «Лаборатория Касперского», которая провела совместное расследование с Европолом и Интерполом. Хакерская атака длилась в течение двух лет.

Кибератаки на атомные станции

Множество гражданских ядерных объектов по всему миру подвержены риску хакерских атак, уверены специалисты британского аналитического центра Chatham House. Многие АЭС не готовы к защите от подобного рода угроз, а устройство сетей отдельных ядерных объектов даже можно найти в Интернете [6].

Инцидент с АЭС «Дэвис-Бесс» в Огайо произошел в 2003 г., когда программное обеспечение об-

служивающей АЭС компании было заражено вирусом Slammer, который привел к отказу серверов корпоративной сети. Оператор совершил ошибку и в ходе расследования инцидента подключил корпоративную сеть к внутренней компьютерной сети станции, и вирус распространился дальше, что сделало невозможным использование компьютеров сотрудниками самой АЭС, которые потеряли связь друг с другом. Также на шесть часов была выведена из строя система отображения параметров безопасности, которая показывает операторам, как работает оборудование и насколько оно исправно.

Серьезный случай произошел в 2006 г. на АЭС «Браунс Ферри» в Алабаме, когда главная система безопасности АЭС оказалась перегруженной сетевым трафиком, что едва не привело к опасной аварии.

В декабре 2014 г. серьезный общественный резонанс вызвал взлом южнокорейского оператора АЭС Hydro and Nuclear Power Co Ltd. Хакер разослал 5986 содержащих вредоносный код электронных писем более чем 3 тыс. сотрудников компании и в итоге получил доступ в ее внутреннюю сеть. Затем злоумышленник через Twitter потребовал заглушить три реактора АЭС, угрожая их разрушением. В итоге он потребовал выкуп под угрозой раскрытия украденной из сети оператора АЭС конфиденциальной информации, однако представители компании заявили, что критически важная информация похищена не была.

6. Кибервойна

В процессе формирования глобального киберпространства происходит конвергенция военных и гражданских компьютерных технологий. В ведущих зарубежных государствах интенсивно разрабатываются новые средства и методы активного воздействия на информационную инфраструктуру потенциальных противников, создаются различные специализированные кибернетические центры и подразделения управления и командования, основной задачей которых является защита государственных и военных информационных инфраструктур, подготовка и проведение активных деструктивных действий в информационных системах противника. Так, собственные официальные кибервойска уже существуют у США, Китая, Англии, Франции, Германии, Израиля и ряда других государств. Противоборство в киберпространстве становится принципиально новой сферой противоборства между государствами [8].

Ведущие мировые державы открыто обсуждают и необходимость защиты от враждебных действий противника в киберпространстве, и планы по наращиванию своих кибермощностей. Это порождает цепную реакцию и вынуждает остальные страны также собирать команды высокопрофессиональных программистов и хакеров (*хакер в переводе с английского означает рубщик (to hack — рубить)*) для разработки специализированных киберсредств — как для защиты, так и для нападения. Гонка кибервооружений набирает обороты.

Принципиальное отличие кибервойны от традиционных военных действий состоит в том, что кибератаки на государственные информационные ресурсы могут вестись негосударственными субъектами. Кибервойна — это не только продолжение политики иными средствами, но и продолжение войны иными средствами. Стратегические цели кибервойны те же — вывод из строя важнейших инфраструктурных, финансовых и правительственных объектов противника.

Всемирный экономический форум (ВЭФ) опубликовал доклад «*Глобальные риски 2015*» (Global Risk Report 2015), на многих страницах которого можно встретить упоминание кибератак и угроз кибербезопасности. Кибератаки вошли в число десяти ведущих глобальных рисков с точки зрения вероятности, а их последствия — в число десяти ведущих глобальных рисков с точки зрения воздействия.

Уже в 2016 г. доклад ВЭФ вводит риски киберпространства в число четырех основных долгосрочных геополитических рисков. Причем риски киберпространства в ближайшее время способны затмить все остальные, потому что границы и армии не могут их ограничить. Особую угрозу представляют вредоносные программы для критической инфраструктуры — электросетей, авиадиспетчерских систем, нефтепроводов, водоснабжения, финансовых платформ и так далее, и не обязательно, что государства должны быть вовлечены во все это: физические и негосударственные субъекты могут использовать вредоносные программы, просто наняв на работу необходимых специалистов на международном подпольном рынке.

Специальная технология, позволяющая обойти или обмануть системы кибербезопасности, в том

числе те, которые должны защищать такие сверхсекретные промышленные объекты, как АЭС, называется атака «нулевого дня». Она представляет собой определенный вредоносный код, выполняемый перед основной вредоносной программой, и предназначена для использования уязвимости, которая является новой и неизвестной в целевой системе.

Атака «нулевого дня» способна полностью или временно вывести из строя систему управления кибербезопасностью и таким образом открыть целевую компьютерную систему для внедрения и начала работы основной вредоносной программы. Многие высококвалифицированные хакеры усердно работают над обнаружением новых уязвимостей в системах, которые позволяют создавать новые атаки «нулевого дня». Мотивацией для этих хакеров является то, что атаки «нулевого дня» можно дорого продать государствам или экстремистам. Атаки «нулевого дня», обнаруженные и разработанные высококвалифицированными хакерами, являются важной составляющей существующего поколения кибероружия.

В международном договоре между Правительством Российской Федерации и Правительством Китайской Народной Республики закреплено понятие «*компьютерная атака*», которое трактуется как «целенаправленное воздействие программными (программно-техническими) средствами на информационные системы, информационно-телекоммуникационные сети, сети электросвязи и автоматизированные системы управления технологическими процессами, осуществляемое в целях нарушения (прекращения) их функционирования и (или) нарушения безопасности обрабатываемой информации» [10].

Кибератака представляет собой преднамеренные действия по изменению, разрушению, искажению, запрещению, нарушению или уничтожению информации и программ, находящихся в компьютерных системах и сетях, или самих компьютеров и сетей.

Спецификой кибервойны являются относительно низкие затраты по сравнению с обычными военными действиями. К примеру, стоимость производства современного атомного авианосца — порядка 5 млрд долл., стоимость его годовой эксплуатации — 160 млн долл. Стоимость кибератаки, способной вывести из строя программное обеспечение (ПО) крупного военного объекта, — менее 5 млн долл. Иногда существенно меньше.

«Вывод из строя любого компьютера, отвечающего за работу ядерных и химических предприятий, будет равносилен поражению части территории нашей страны ядерной бомбой», — заявил не так давно экс-министр обороны США Леон Панетта [8].

Кибератаки могут проводить и террористические группировки — кибертерроризм. Кибертерроризм может быть определен как использование компьютеров в качестве оружия или целей политически мотивированными международными или национальными группами или тайными агентами, причиняющими или угрожающими причинить ущерб и посеять панику, с целью воздействия на население или правительство для изменения политики.

Объектом нападения необязательно должен быть крупный военный или гражданский объект. Им может быть информационная система. Достаточно вывести из строя три-четыре крупнейших банка какой-нибудь европейской страны, и финансовая система этого государства окажется в коллапсе.

Сегодня становится ясно, что для сохранения суверенитета государство должно не только отстаивать социально-экономические и политические интересы, но и тщательно охранять свое информационное пространство. И теперь едва ли не на первый план выступает задача контролировать критически важные для государства информационные системы.

Устав ООН предусматривает руководящие принципы для обоснования ответных действий на кибератаки, являющиеся применением силы. Они приведены в статье 2 (4) — разрушительные действия, подходящие под определение «применение силы», и в статье 51 — разрушительные действия, подходящие под определение «вооруженного нападения», несущие угрозу государственному суверенитету.

Наиболее опасными мишенями кибератак являются в первую очередь ключевые системы информационной инфраструктуры (КСИИ), управляющие критически важными объектами. Для управления объектами в КСИИ используется то или иное программное обеспечение, не лишенное ошибок и уязвимостей.

Вывод из строя таких объектов может привести к хаосу и катастрофам. Наша жизнедеятельность так или иначе зависит от этих систем. Они обогревают наши дома, подают в них воду и электричество, обеспечивают радио- и телевещание,

управляют транспортными потоками, контролируют добычу ресурсов и производственные процессы на фабриках и заводах.

Помимо промышленных объектов существует множество организаций, для которых несанкционированный доступ к информации может стать серьезной проблемой: банки, медицинские и военные учреждения, исследовательские институты и бизнес.

Кибероружие становится опаснее ядерного. Под кибероружием следует понимать технические и программные средства поражения (устройства, программные коды), которые конструктивно предназначены для воздействия на программируемые системы, эксплуатацию уязвимостей в системах передачи и обработки информации или программно-технических системах, с целью уничтожения людей, нейтрализации технических средств либо разрушения объектов инфраструктуры противника. Данное понятие может быть соотнесено с более общим понятием «информационное оружие».

В июне 2013 г. президенты РФ и США Владимир Путин и Барак Обама поручили установить линию прямой связи по вопросам урегулирования ситуаций, создающих угрозу кибербезопасности, используя в этих целях линию прямой связи между центрами по уменьшению ядерной опасности США и России [http://tass.ru/mezhdunarodnaya-panorama/617111].

Характерными чертами кибероружия являются: 1) отсутствие физического вмешательства при воздействии на систему; 2) эксплуатация уязвимостей внутри конкретной системы (или определенного типа систем); 3) точно предустановленный результат комплексов, воздействующих по установленным алгоритмам.

Киберсредства поражения представляют собой *вирусы*. Для вирусных атак уязвимы все компьютерные операционные системы. Пути попадания вирусов в компьютеры различны, но общее в них одно — вирусы входят в компьютерные системы только из внешних источников. Известны несколько различных форм вирусов, которые могут вторгнуться в компьютерную систему. В настоящее время существует 3 основные категории вредоносных ПО: вирусы, черви и трояны («троянский конь»).

В принципе, любое киберсредство является специальной программой, разработанной в единичном экземпляре и предназначенной для однократного использования при осуществлении конкретной операции. Первым общеизвестным вредоносным боевым кодом, использовавшимся как кибероружие, стал червь Стакснет (Stuxnet). Червь был запрограммирован на распространение через USB, что позволяло вторгаться в защищенные от воздействия из мировой сети объекты. Также он имел подробный алгоритм создания и загрузки своих модулей в атакуемую систему в зависимости от работы на компьютере определенных защитных решений. Таким образом Stuxnet старался свести к минимуму воздействие на заведомо защищенную достаточным образом систему во избежание обнаружения.

«Лаборатория Касперского» за последние несколько лет нашла уже 4 боевых вируса. Изучение этих вирусов показало, что они созданы отнюдь не группой частных лиц, чтобы воровать персональные данные, деньги с кредитных карт. Это вирусы, созданные на государственном уровне. Стоимость разработки одного или двух таких вирусов в «Лаборатории Касперского» оценили в 100 млн долл. Этого не может себе позволить ни одна группа хакеров. Кроме того, вирусы настолько сложные, что совершенно очевидно, что их много лет разрабатывало много людей очень высокой квалификации.

В 2013 г. «Лабораторией Касперского» была опубликована информация о совершенно новом явлении в области компьютерных атак. Была раскрыта шпионская сеть «Красный Октябрь» (Red October), на протяжении пяти лет занимающаяся хищением государственных секретов. Это сложнейший комплекс вредоносных программ, около 1000 вредоносных файлов, относящихся к 30 различным группам модулей.

Информатизация общества постоянно создает новые потенциальные цели для кибероружия. Любое медицинское учреждение с тяжелым оборудованием вроде томографов способно стать жертвой специально разработанного вредоносного кода, отдельные электростанции и даже системы ПВО могут быть выведены из строя по невнимательности или злому умыслу. Разумеется, подобные объекты становятся целью кибератаки в случае полномасштабной войны или террористического акта, но кибервойна может быть и экономической.

Кибервойна из фазы проверки противника на уязвимость может решительно перейти к стадии нанесения полномасштабных кибердаров по экономическим и военным объектам, всем объектам критической инфраструктуры, от которых зависит сама жизнеспособность, безопасность государств, общественная стабильность. Кибервойны могут оказаться не менее разрушительными и жестокими по сравнению с так называемыми обычными. При этом еще надо делать поправку на трансграничный и всепроникающий характер информационных технологий и соответствующего оружия.

Военное руководство США рассматривает борьбу в киберпространстве как составную часть информационного противоборства, которое должно вестись не только в четырех традиционных пространствах — наземном, морском, воздушном и околоземном космическом, но и в киберпространстве. Еще в 2008 г. министерство обороны США определило противоборство в киберпространстве как оперативно-стратегическую категорию, характеризующую процесс соперничества конфликтующих сторон, в котором каждая проводит в отношении другой операции, мероприятия или акции, связанные с программно-математическим и другими видами воздействия на объекты системы боевого управления и связи противника, его оружие и военную технику в интересах решения поставленных задач.

В целом кибероружие предназначено для решения следующих задач:

- временное отключение от компьютерной сети критически важных узлов коммуникационной инфраструктуры;
- блокирование компьютерных операций и функций;
- нарушение работы и вывод из строя автоматизированных систем управления и связи;
- искажение и фальсификация информации, распространение дезинформации.

США на официальном уровне заявляют, что готовы на кибернападение ответить всеми имеющимися в их распоряжении средствами. По американским данным, более 120 стран в современном мире экспериментируют в области кибервойны. К этому нужно добавить преступников и террористов в области использования ИКТ, так называемый субъективный фактор в лице отдельных хакеров.

7. Кибербезопасность

В XXI веке кибербезопасность начинает выступать как основной фактор национальной и международной безопасности [7, 14].

Кибербезопасность (философское определение) — это свойство или состояние системы сохранять надежность и функциональную устойчивость в условиях современного информационного противоборства.

Кибербезопасность (определение по технической сущности) — информационная безопасность компьютерных информационно-управляющих систем, обеспечивающая их высокую надежность и функциональную устойчивость в условиях современного информационного противоборства.

Россия как одно из ведущих государств мира является первоочередным объектом для негативных кибервоздействий в стремлении других стран к мировому лидерству. В настоящее время существует потенциальная угроза нарушения функционирования критически важных информационных систем основных объектов жизнеобеспечения государства, ВС РФ, МВД, ФСБ, ФСО, МЧС России при массированном воздействии компьютерных атак на их уязвимости. При этом прежние базовые информационные защищенные компьютерные технологии и традиционные средства защиты информации недостаточны и уже не обеспечивают необходимого уровня защищенности и функциональной устойчивости.

Нормативное обеспечение кибербезопасности

Актуальность проблемы кибербезопасности признается на высшем уровне руководства государства и определена в следующих регламентирующих документах в области защиты КВО и КСИИ.

1. «*Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации*» (документ Совета безопасности, утвержденный Президентом Российской Федерации 3 февраля 2012 г. № 803).

Целью государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфра-

структуры Российской Федерации является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства.

К 2020 г. должен быть обеспечен:

• ввод в эксплуатацию Ситуационного центра единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру Российской Федерации и оценки уровня реальной защищенности ее элементов и ситуационных центров регионального и ведомственного уровней;

• ввод в эксплуатацию в целом единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов.

В период после 2020 г. должен осуществляться комплекс мероприятий по поддержанию организационной, экономической, научно-технической и технологической готовности Российской Федерации к предотвращению угроз безопасности ее критической информационной инфраструктуры.

2. Указ Президента РФ от 15 января 2013 г. № 31с *«О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»*. Для ознакомления была опубликована открытая выписка из Указа Президента, согласно которой:

• на ФСБ России возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом;

• определены основные задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

• полномочия ФСБ России в части:

– разработки методики обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами — на иные информационные системы и информационно-телекоммуникационные сети;

– определения порядка обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации;

– организации и проведения мероприятий по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

– разработки методических рекомендаций по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак.

3. Указ Президента РФ от 22 мая 2015 г. № 260 *«О некоторых вопросах информационной безопасности Российской Федерации»* [http://base.garant.ru/71035416/#block_1000#ixzz4K2WDys6u].

«В целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети Интернет на территории Российской Федерации постановляю:

1. Преобразовать сегмент международной компьютерной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны Российской Федерации, в российский государственный сегмент информационно-телекоммуникационной сети "Интернет", являющийся элементом российской части сети "Интернет" и обеспечивающий:

а) подключение к сети "Интернет" предназначенных для взаимодействия с ней государственных информационных систем и информационно-телекоммуникационных сетей государственных органов, а также информационных систем и информационно-телекоммуникационных сетей организаций, созданных для выполнения задач, поставленных перед федеральными государственными органами;

б) размещение (публикацию) в сети "Интернет" информации государственных органов и названных в подпункте "а" настоящего пункта организаций.

4. Администрации Президента Российской Федерации, Аппарату Правительства Российской Федерации, Следственному комитету Российской Федерации, федеральным органам исполнительной власти и органам исполнительной власти субъектов Российской Федерации осуществить до 31 декабря 2017 г. подключение находящихся в их ведении государственных информационных систем и информационно-телекоммуникационных сетей к российскому государственному сегменту сети "Интернет" и обеспечить размещение (публикацию) информации в сети "Интернет" в соответствии с порядком, утвержденным настоящим Указом.

5. Рекомендовать Совету Федерации Федерального Собрания Российской Федерации, Государственной Думе Федерального Собрания Российской Федерации, судебным органам Российской Федерации, органам прокуратуры Российской Федерации, Счетной палате Российской Федерации, а также организациям, созданным для выполнения задач, поставленных перед федеральными государственными органами, осуществить подключение находящихся в ведении названных органов и организаций информационных систем и информационно-телекоммуникационных сетей к российскому государственному сегменту сети "Интернет" и обеспечить размещение (публикацию) информации в сети "Интернет" в соответствии с порядком, утвержденным настоящим Указом.

Подключение информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" через российский государственный сегмент сети "Интернет" осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств.

Защита информации в информационных системах и информационно-телекоммуникационных сетях, подключаемых к сети "Интернет" через российский сегмент, в том числе с использованием средств государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, обеспечивается в соответствии с законодательством Российской Федерации».

4. В настоящее время ведется и находится на стадии завершения работа по согласованию следующих проектов документов:

- проект Федерального закона «*О безопасности критической информационной инфраструктуры Российской Федерации*».

Проектом определяются цели и принципы обеспечения безопасности критической информационной инфраструктуры Российской Федерации, полномочия органов государственной власти в этой сфере, порядок категорирования объектов критической информационной инфраструктуры и оценки их защищенности, источники финансирования мероприятий по обеспечению безопасности.

В законопроекте определяются такие понятия, как информационные ресурсы РФ, компьютерная атака, компьютерный инцидент, критически важный объект, критическая информационная инфраструктура РФ, субъекты критической информационной инфраструктуры РФ и ряд других.

Документ также предусматривает разработку критериев отнесения объектов критической информационной инфраструктуры к различным категориям опасности и установление требований к системам безопасности данных объектов;

- проект закона, вносящий поправки в Федеральный закон «*О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"*».

5. ГОСТ РО 0043-001-2010 «Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения».

6. Федеральной службой по техническому и экспортному контролю (ФСТЭК) России разработан пакет руководящих документов (РД) по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, включающий:

- «Базовую модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Методику определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);

• «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007);

• Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

В 2013 г. организованы работы по созданию Национального центра управления обороной государства (НЦУОГ), предназначенного для решения задач контроля и управления всеми силами и средствами, действующими в интересах обороны страны как в военное, так и в мирное время, в том числе и системой кибербезопасности России. В том же году принято решение и организованы работы по созданию в Минобороны России киберкомандования для защиты общенациональных интересов в киберпространстве.

В Стратегии развития отрасли информационных технологий в Российской Федерации на 2014—2020 гг. и на перспективу до 2025 г. включен раздел по обеспечению информационной безопасности:

«*Учитывая масштабы проникновения информационных технологий в повседневную жизнь граждан, организаций и органов власти всех уровней, а также высокий уровень зависимости создаваемых в стране информационных систем от импортной продукции, особенно актуальным становится вопрос обеспечения должного уровня информационной безопасности страны в современном глобальном информационном мире. В этих условиях необходимо предпринять меры, направленные на обеспечение информационной безопасности не только государственных органов власти, но и других организаций и граждан, проживающих на территории России*».

25 марта 2015 г. на сайте ФСБ России была опубликована выписка из *Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации*, в которой описывается государственная Система обнаружения, предупреждения и ликвидации последствий компьютерных атак (СОПКА). Концепция была принята Указом Президента от 12 декабря 2014 г. № К 1274, а в выписке есть ссылка на Указ Президента от 15 января 2013 г. № 31с «*О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации*», который и определяет основные цели и задачи СОПКА.

В выписке говорится: «*Система представляет собой единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования Системы*».

В сентябре 2016 г. стало известно, что в ближайшее время в России заработает центр реагирования на инциденты в сфере информационной безопасности (CERT), созданный «Лабораторией Касперского» для сбора информации об уязвимостях и отражении атак на такие объекты, как атомные электростанции, предприятия ядерно-топливного, нефтегазового и энергетического комплексов. CERT-GIB (Computer Emergency Response Team — Group-IB) — центр круглосуточного реагирования на инциденты информационной безопасности.

CERT будет собирать информацию о найденных уязвимостях, угрозах, инцидентах, а также привлекаться к проведению обследований, тестов на проникновение и расследований инцидентов на промышленных объектах.

Заключение

В настоящее время риски киберпространства приобретают все больший вес и обеспечение кибербезопасности становится серьезной задачей для любого развитого государства. Атаки на промышленные системы стали важнейшей угрозой, которая носит глобальный характер и представляет опасность не только для экономики, но и для безопасности обеспечения жизнедеятельности населения.

Актуальность темы цифрового суверенитета РФ продолжит расти, особенно в связи с обострением в отношениях с Западом и введением санкций в отно-

шении России. Отсюда — приоритетность информационной безопасности критически важных объектов.

Проблема кибербезопасности в нашей стране стоит особенно остро во многом из-за слабой нормативно-правовой базы. Фактически сформулированный и закрепленный целостный подход к национальной проблематике кибербезопасности на сегодняшний день отсутствует.

Сегодня все больше предприятий понимают серьезность киберугроз, более того, киберугрозы, например, критической энергетической инфраструктуре признаются реальными на уровне регулирующих органов. Например, в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 31 декабря 2015 г., обращается внимание на угрозы критической информационной инфраструктуре Российской Федерации.

МЧС России в Прогнозе чрезвычайной обстановки на территории Российской Федерации на 2016 г. от 24.12.2015 г. выделяет кибертерроризм относительно энергетических объектов России. В прогнозе отмечается, что в настоящее время уровень информационной безопасности не соответствует уровню угроз в данной сфере и в 2016 г. возможно повышение числа хакерских атак с целью создания условий для возникновения техногенных ЧС. Отмечается, что из промышленных объектов наиболее уязвимы при хакерских атаках энергетические и коммуникационные сети России.

Литература

1. Шапинская Е. Н. Человек XXI века на просторах киберпространства: безграничные возможности и новые опасности. http://gigabaza.ru/doc/4749.html
2. Развитие интернета в регионах России. Весна 2016. https://yandex.ru/company/researches/2016/ya_internet_regions_2016
3. Защита ключевых систем информационной инфраструктуры. http://ace-net.ru/security/sec-facility.html
4. Царев Е. Нормативная база защиты критически важных объектов (КВО). http://www.securitylab.ru/blog/personal/tsarev/23617.php
5. Безопасность ключевых систем информационной инфраструктуры: точка доверия. https://securelist.ru/analysis/obzor/131/bezopasnost-klyuchevy-h-sistem-inform/
6. Пискунова Н. Кибербезопасность и атомная энергетика: все еще предстоит // Индекс безопасности. 2014. № 1 (108). Т. 20.
7. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века. Ч. 1 // Вопросы кибербезопасности. 2013. № 1.
8. Неманья Никитович. Стратегия и тактика кибервойн: в ожидании серьезных межгосударственных конфликтов // Information Security/Информационная безопасность. 2013. № 5.
9. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. 2013 г. www.scrf.gov.ru/documents/6/114.html
10. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, 8 мая 2015 года, Москва.
11. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.
12. Цирлов В. Л. Правовые основы кибербезопасности Российской Федерации // Правовая информатика. 2014. Вып. № 3.
13. Кибербезопасность и управление Интернетом: Документы и материалы для российских регуляторов и экспертов / Отв. ред. М. Б. Касенова. М.: Статут, 2013.
14. Клименский М. М. Кибербезопасность: существующие угрозы и проблемы ее обеспечения на современном этапе. https://pglu.ru/upload/iblock/70f/kiberbezopasnost-sushchestvuyushchie-ugrozy-i-problemy-ee-obespecheniya-na-sovremennom-etape.pdf

Сведения об авторе

Соколов Юрий Иосифович: старший научный сотрудник 6 Центра ФГУ ВНИИ ГОЧС (ФЦ) МЧС России

Число публикаций: более 200

Область научных интересов: риски ЧС и высоких технологий

Контактная информация:

Адрес: 121352, г. Москва, ул. Давыдковская, д. 7

Тел.: +7(495) 413-84-50

E-mail: soko-718@rambler.ru