УДК 004.491 + 004.056

ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ ОТ КИБЕРАТАК

Л.М. Пысина, А.А. Пыринов, В.Ю. Бердюгин

В данной статье ставится задача рассмотреть фундаментальные проблемы защиты информационных объектов от кибератак. На основе нормативно-правовой базы России проанализированы методы защиты информации в настоящее время. Выявлена и обоснована необходимость введения нового законопроекта. По итогам проведенного исследования авторами предлагается ряд решений по усовершенствованию обеспечения кибербезопасности в России.

Ключевые слова: информация, информационный объект, информационная безопасность, кибербезопасность, кибератака, киберпреступление, терроризм, кибертерроризм.

Кибератака – целенаправленное воздействие на информационные ресурсы программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих ресурсах. [1] Актуальность проблемы защищённости информационных объектов от кибератак обуславливается уровнем развития цифровой среды, первой основополагающей тенденцией которой является информационный взрыв. В последнее время объем информации удваивается каждые два года. По данным компании

Cisco объем сгенерированных данных в 2012 году составил 2,8 зеттабайт и увеличится до 40 зеттабайт к 2020 г. Примерно треть передаваемых данных составляют автоматически сгенерированные данные, т.е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к Интернету. [2]

Рост информатизации общества способствует и росту числа киберпреступлений – совершаемых в сфере информационных процессов и посягающих на информационную безопасность деяний, предметом которых являются информация и компьютерные средства.

По данным исследования, проведенного Фонда Развития Интернет-Инициатив, а также компаниями Group-IB и Microsoft, общий ущерб от кибератак за 2015 год составил для экономики РФ 203,3 млрд рублей. Кроме прямого ущерба (оценивается в 123,5 млрд рублей), 79,8 млрд рублей пришлось на затраты на ликвидацию последствий инцидентов в области информационной безопасности [3].

В последние годы всё больше внимания уделяется кибертерроризму – предумышленному совершению действий, нарушающих функционирование компьютеров и/или телекоммуникационных сетей, либо угрозе совершения таких действий, с намерением причинить вред или совершённой по социальным, идеологическим, религиозным или политическим мотивам; а также угрозам личного характера, совершённым по тем же мотивам [4].

Первой известной кибертеррористической атакой является отключение Массачусетского провайдера и повреждение части его системы учёта одним из сторонников идеологии «белого супермасизма» – превосходства белой расы. Атака была совершена в 1996 году, после того, как провайдер попытался предотвратить рассылку по всему миру рассылку расистских писем. Хакер, устроивший атаку, оставил сообщение следующего содержания: «You have yet to see true electronic terrorism. This is a promise» – «Вы ещё увидите настоящий электронный терроризм. Я обещаю».

Конечно, говорить сейчас о глобальной угрозе кибертерроризма пока еще рано – террористические организации пока предпочитают совершать теракты «по старинке», используя информационные технологии лишь в качестве средства связи, однако, возможность захвата критически важных объектов существует уже сейчас. Ярким примером такого теракта является высвобождение Витеком Боденом, недовольным сотрудником водоочистительной компании, более 800000 литров неочищенных сточных вод в реку Маркучи в Австралии в 2000 году [5].

Следует различать понятия обеспечения информационной безопасности и кибербезопасности. Если в процессе обеспечения информационной безопасности, объектом защиты является информация, которая обрабатывается, передается и хранится в автоматизированных системах, а основная цель – обеспечение ее конфиденциальности, то в процессе обеспечения кибербе-

зопасности защищаемым ресурсом, в первую очередь является сам технологический процесс, а основной целью – обеспечение его непрерывности (доступности всех узлов) и целостности. Термин «кибербезопасность» используется в основном применительно к автоматизированным системам управления технологическим процессом, поле потенциальных рисков и угроз для которых, по сравнению с корпоративными системами, расширяется рисками потенциального ущерба жизни и здоровью персонала и населения, ущербу окружающей среде и инфраструктуре [6].

Анализ состояния кибербезопасности России показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Для обеспечения информационной безопасности сейчас создана целая система нормативных документов. В России к нормативно-правовым актам в области информационной безопасности относятся:

- Конституция РФ;
- Международные договоры РФ;
- Законы федерального уровня;
- Указы Президента РФ;
- Постановления Правительства РФ;
- Нормативные правовые акты федеральных министерств и ведомств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и т.д. [7]

Если же говорить о кибербезопасности, то подобная система нормативно-правовых документов не полностью разработана.

В 2013 году была принята Концепция Стратегии кибербезопасности России, которая обосновала необходимость и своевременность разработки Стратегии кибербезопасности России, определяла ее принципы и направления, а также ее место в системе нормативных актов государства [8]. Однако, сама Стратегия до сих пор не разработана.

В 2014 году издан приказ ФСТЭК 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» [9]. Данный нормативный документ позволил урегулировать некоторые вопросы в области обеспечения кибербезопасности на критически важных объектах: он установил критерии отнесения объектов критической информационной инфраструктуры (совокупность автоматизированных систем управления КВО и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления; обеспечения обороноспособности, безопасности и

правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий [10]) к различным категориям опасности; требования к системам безопасности объектов критической информационной инфраструктуры.

Это, безусловно, важный шаг на пути обеспечения кибербезопасности, но одного этого приказа недостаточно. Необходимы документы, определяющие орган власти, который должен следить за соблюдением данных требований, наказание за их несоблюдение. Существующее регулирование не охватывает в необходимой мере систему отношений, возникающих в рамках киберпространства.

В первую очередь, следует принять закон, который бы регулировал и устанавливал ответственность за несоблюдение мер по обеспечению кибербезопасности критически важных объектов, а также определял орган исполнительной власти, который бы осуществлял контроль за соблюдением данных мер. Принятие подобного закона позволит создать правовую и организационную основу для эффективного функционирования системы безопасности критической информационной инфраструктуры России, направленной, в первую очередь, на предупреждение возникновения компьютерных инцидентов на ее объектах.

Кроме того, для обеспечения эффективной системы противодействия кибератакам, необходимо продолжить политику импортозамещения в сфере технических и программных средств обеспечения кибербезопасности. Данная мера позволит отказаться от закупки импортной техники и программного обеспечения, что, в свою очередь, снизит вероятность несанкционированного доступа, и уменьшит зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

Библиографический список

1. Проект федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» // Консультант-плюс. – URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=109240;div=PRJ;dst=100006/.

2. Ларина, Е. Кибервойны XXI века. Возможности и риски для России / Е. Ларина, В. Овчинский. – М.: Книжный мир, 2014. – С. 7.

3. Потери экономики РФ от киберпреступности оценили в 123,5 млрд рублей // Интерфакс. – URL: http://www.interfax.ru/business/503554/.

4. Компьютерный терроризм // Википедия. – URL: https://ru.wikipedia.org/wiki/Компьютерный_терроризм/.

5. Cyberterrorism // Wikipedia. – URL: https://en.wikipedia.org/wiki/Cyberterrorism/.

6. Кибербезопасность АСУ ТП – что это и зачем? // Диалогнаука. – URL: http://www.dialognauka.ru/press-center/article/13226/.

7. Бачило, И.Л. Актуальные проблемы информационного права / И.Л. Бачило, М.А. Лапина. – М.: Юстиция, 2016. – С. 55.

8. Концепция Стратегии кибербезопасности Российской Федерации // Совет Федерации Федерального Собрания Российской Федерации. – URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf/.

9. Приказ ФСТЭК России от 14 марта 2014 г. N 31 // ФСТЭК России. – URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31/.

10. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. – URL: http://www.scrf.gov.ru/documents/6/113.html/.

К содержанию