Педанова Полина Васильевна

магистрант

ФГБОУ ВО «Пятигорский государственный университет»

г. Пятигорск, Ставропольский край

КИБЕРПРЕСТУПНОСТЬ КАК ФАКТОР ВОЗНИКНОВЕНИЯ КОНФЛИКТНЫХ ВЗАИМООТНОШЕНИЙ МЕЖДУ ГОСУДАРСТВАМИ

***Аннотация**: в статье рассмотрены тенденции развития киберпреступности, изучены подходы к данной проблеме. Кроме того, в тексте изложены примеры влияния преступлений в сети Интернет на развитие отношений между развитыми государствами.*

***Ключевые слова**: кибербезопасность, коммуникация, Интернет, веб-технологии, хакерские атаки.*

Век информационных технологий ознаменован появлением новых форм коммуникации. Глобальная сеть Интернет, прочно обосновавшаяся в жизни современного человека, помимо достоинств, очевидно, имеет и ряд недостатков, порой влияющих на ход ряда общественных процессов. С наступлением 2000-х годов в обиход граждан входят технические термины, понятия, касающиеся веб-технологий. Появившийся простор для деятельности в виде интерактивного пространства позволяет не только успешно удаленно работать, но и совершать преступления. В последние два десятилетия всю большую популярность набирает явление киберпреступности.

Киберпреступность – любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках сети Интернет или против компьютерной системы или различных сетей. Следовательно, к данному виду преступлений могут быть отнесены любые действия, относящиеся по своим характеристикам к понятию «преступление», но совершенное в веб-среде.

По данным международной исследовательской компании Allianz Global Corporate & Specialty, в 2016 году общий ущерб от проступков, выявленных в Интернет-пространстве, составил для мировой экономики более 575 миллиардов

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

долларов, порядка 1% мирового ВВП. Рейтинг мировых держав, понесших потери от действий сетевых преступников, в порядке убывания складывается следующим образом: 1-е место занимает Германия, далее – США, Китай и Российская Федерация. По данным Фонда развития интернет-инициатив (ФРИИ), наша страна потерпела ущерб от кибернарушений в 2016 году в размере более 200 миллиардов рублей, а также понесла затраты на восстановление систем и ликвидацию последствий порядка 80 миллиардов [1].

Тенденции последних десятилетий указывают на широкое распространение киберугроз в мире. Причем, они начинают затрагивать не только интересы коммерческих компаний, индивидуальных предпринимателей и обычных пользователей, но и становятся объектом дискуссий в мировом сообществе.

Среди причин возникновения напряженности, предконфликтных и даже конфликтных отношений между государствами появляется активность в киберпространстве. Этим обусловлено включение данного направления в перечень основных угроз, стоящих перед мировым сообществом. С 2007 года Американский Совет по международным отношениям выделяет конфликты, требующие усиленного внимания на мировой арене. В 2017 году они будут представлять собой две группы: первая – ситуации, которые могут повлиять на обстановку в мире, вторая – конфликты с меньшим влиянием, но находящиеся на стадии формирования с высокой вероятностью эскалации. Кибератаки, которые наносят серьезный ущерб экономике государств, отнесены к первой группе проблемных вопросов наравне с террористическими атаками.

Конец 2016 года был ознаменован заявлениями правительства Соединенных Штатов Америки о причастности России к взлому сервера национального комитета Демократической партии США. За данными объявлениями последовали действия по введению санкций в отношении ФСБ России, ГРУ и нескольких других организаций, безосновательно признанных причастными к вышеописанному инциденту. Данные действия признаны Правительством Российской Федерации необоснованными, названы «охотой на ведьм». 6 января была обнародо-

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

вана часть доклада разведки США, в котором ЦРУ, ФБР и АНБ заявили, что Президент России Владимир Путин отдал приказ о запуске «кампании влияния» на президентские выборы в США [2]. Секретная часть доклада была представлена 5 января действующему президенту США Бараку Обаме, а затем – будущему главе государства Дональду Трампу. Позднее список пополнили серверы национального комитета республиканцев, Пентагона. Брифинг разведывательных служб США продемонстрировал согласие избранного президента с заявлениями о том, что Россия, Китай и ряд других стран покушались на киберзащиту государственных институтов и других организаций, хотя отказался признать главенствующую роль России в данных действиях.

Сложившаяся ситуация послужила толчком к развязыванию предконфликтной ситуации между Россией и США, но конфликта не произошло. Разведывательные службы Америки на настоящий момент так и не предоставили объективных доказательств причастности российских хакеров к произошедшим атакам. Аргументы начальника пресс-службы Госдепартамента США Джона Кирби сводятся к тому, что доказательства не обнародуются в связи с опасениями утечек дополнительной информации о методах работы американских спецслужб [3].

Данная проблема существует и в Европе. В январе 2017 года Федеральная служба защиты конституции Германии выступила с официальными выступлениями о том, что есть вероятность причастности хакеров из России к атаке на информационные системы Организации по безопасности и сотрудничеству в Европе. По данным Financial Times, также серверы Еврокомиссии все чаще в последнее время подвергаются кибератакам [4].

В связи с участившимися случаями хакерских атак, в развитых государствах ведется активная политика по противодействию данным процессам: шифрование данных, расширение сотрудничества по вопросам кибербезопасности с крупными международными организациями и союзами, финансирование кибервойск. По данным Zecurion Analytics, численность кибервойск в США составляет 9000 человек, в России и Германии – 1000, Китае – 20000 [5; 6].

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Процесс формирования кибервойск стал особенно актуальным ввиду подсчетов последних данных. На форуме по информационной безопасности «Инфофорум-2017» заместителем начальника Центра ФСБ России Николем Мурашовым были обнародованы следующие цифры: по всему миру за последние годы ущерб от кибератак от 300 миллиардов до одного триллиона долларов по разным методикам оценки [7].

Правительство Российской Федерации рассматривает вопрос об ужесточении наказания в отношении лиц, совершивших преступления в веб-среде. Это связано с тем, что сейчас суммы ущерба значительно превышают срок наказаний, который составляет в нашей стране 5 лет. Для сравнения, в Китае преступник получит от 10 лет лишения свободы, в США – 25 лет. Поэтому планируется создание такого законопроекта, который признает киберпреступления кражей, соответственно увеличит сроки отбывания наказаний.

Сложившаяся на международной арене ситуация в отношении противостояния кибератакам демонстрирует остроту данной проблемы. Между тем, эксперты прогнозируют усугубление положения, увеличение числа и повышение профессионального уровня хакерских преступлений. Подвергнутся нападению информационные системы и информационно-телекоммуникационные сети органов государственной власти, автоматизированные системы управления технологическими процессами в разных отраслях: энергетике, здравоохранении, связи, финансах, металлургии и других.

Список литературы

1. Аналитический отчет Фонда развития Интернет-инициатив за 2016 год [Электронный ресурс]. – Режим доступа: http://www.iidf.ru/

2. Joint Statement from the ODNI and the DOJ on the Declassification of Renewal of Collection Under Section 501 of the FISA. – 2017, 6 January [Электронный ресурс]. – Режим доступа: https://www.dni.gov/index.php/newsroom/press-releases/224-press-releases-2017/1466-odni-statement-on-declassified-intelligence-community-assessment-of-russian-activities-and-intentions-in-recent-u-s-elections (дата обращения: 6.01.2017).

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

3. Глава пресс-службы Госдепа вышел из себя из-за вопроса RT о Сирии [Электронный ресурс]. – Режим доступа: http://tass.ru/mezhdunarodnaya-panorama/3790706h (дата обращения: 17.11.2016).

4. Аналитический отчет отдела по информационной безопасности Financial Times [Электронный ресурс]. – Режим доступа: https://www.ft.com/ content/3a0f0640-d585–11e6–944b-e7eb37a6aa8e

5. Коломыченко М. В интернет ввели кибервойска [Электронный ресурс]. – Режим доступа: http://www.kommersant.ru/doc/3187320

6. Доклад Тринадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию № A/CONF.222/L.6 [Электронный ресурс]. – Режим доступа: https://documents-dds-ny.un.org/ doc/UNDOC/LTD/V15/021/22/PDF/V1502122.pdf?OpenElement (дата обращения: 31.03.2015).

7. Итоги Инфофорума-2017 [Электронный ресурс]. – Режим доступа: https://infoforum.ru/news/itogi-infoforyma-2017

8. Боташева А.К. Международный терроризм: проблемы концептуализации // Вестник Пятигорского государственного лингвистического университета. – 2011. – №4. – С. 413–416.

9. Старовойтов А.В. Кибербезопасность как актуальная проблема современности // Информатизация и связь. – 2011. – №6. – С. 4–7.

10. Шариков П.А. Информационный комплекс / П.А. Шариков // Безопасность Европы / Ин-т Европы РАН. – М.: Весь мир, 2011. – С. 581–591.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)