УДК 004.056

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

К. Г. Мамцов, Н. Р. Ачилов
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Киберпреступность представляет опасность для национальной безопасности. Киберпреступники взламывают экономические учреждения, правительственные веб-сайты или энергетические инфраструктуры с целью кражи или вымогательства денег. В данной статье рассматриваются вопросы, связанные с киберпреступностью: анализируется статистика и динамика этого вида преступлений, возможные меры защиты от них.

***Ключевые слова*:** киберпреступность, национальная безопасность, меры предупреждения, компьютерные преступления, кибербезопасность.

CYBERCRIME AS A THREAT TO NATIONAL SECURITY

K. G. Mamtsov, N. R. Achilov
Don State Technical University (Rostov-on-Don, Russian Federation)

Cybercrime poses a threat to national security. Cybercriminals hack into economic institutions, government websites, or energy infrastructures in order to steal or extort money. This article discusses issues related to cybercrime today. The analysis of the dynamics of cybercrime is carried out, the basic provisions in the field of cybercrime are given. Cybercrime statistics are also considered. Possible measures of protection against this type of crime are analyzed.

Keywords: cybercrime, national security, preventive measures, computer crimes, cybersecurity.

Введение. Киберпространство, одно из ответвлений компьютерных и цифровых коммуникационных технологий, в последние десятилетия стало неотъемлемой частью нашей жизни.

Компьютеризация имеет неоценимое значение для оптимизации процессов, связанных с работой, обучением и развлечениями, она затрагивает практически все сферы человеческой деятельности. Как только в 1988 году Интернет стал коммерческим, он быстро превратился в оплот киберпространства, предлагая недорогой и немедленный доступ к источникам информации, широкий обмен информацией, совместную работу на расстоянии и многое другое.

Основная часть. Киберпреступность — это преступная деятельность, целью которой является неправильное использование компьютера, компьютерной сети или сетевого устройства.

Большинство киберпреступлений совершается киберпреступниками, или хакерами, которые зарабатывают на этом деньги. Такая деятельность осуществляется как отдельными лицами, так и организациями. Часто киберпреступники объединяются в организованные группы, которые используют в своей незаконной деятельности передовые технологии и методы, как правило, они обладают высокой технической квалификацией. Киберпреступниками, впрочем, могут быть и начинающие хакеры.

Киберпреступники редко взламывают компьютеры по причинам, не связанным с получением прибыли, например, по политическим или личным.

Последствия киберпреступности для национальной безопасности проистекают из того, как технологии используются враждебными элементами.

Общественный спрос на кибербезопасность растет пропорционально растущему признанию угрозы. Даже в отсутствие объективного увеличения масштабов преступности этот спрос, как ожидается, не уменьшится.

Виды киберпреступности:

1. Мошенничество с электронной почтой и мошенничество в Интернете.

2. Мошенничество с личными данными (кража и злонамеренное использование личной информации).

3. Кража финансовых данных или данных банковских карт.

4. Кража и продажа корпоративных данных.

5. Кибершантаж (требование денег для предотвращения кибератаки).

6. Атаки вымогателей (разновидность киберсаботажа).

7. Криптоджекинг (добыча криптовалюты с использованием чужих ресурсов без ведома их владельцев).

8. Кибершпионаж (несанкционированный доступ к данным государственных или коммерческих организаций).

Большинство киберпреступлений относятся к одной из двух категорий:

— преступная деятельность, целью которой являются сами компьютеры;

— преступная деятельность, в которой компьютеры используются для совершения других преступлений.

В первом случае преступники используют вирусы и другие виды вредоносных программ для заражения компьютеров с целью их повреждения или остановки работы.

Компьютеризация позволяет разбить задачи на небольшие блоки и децентрализовать обработку, сетевое взаимодействие обеспечивает глобальный доступ к информации и фокусируется на знаниях как ценном продукте. Компьютерные технологии внедряются для изменения и повышения эффективности творческих и рабочих процессов во всех аспектах жизни, и мир преступности больше не является исключением [1, с. 98].

Предлагаемое определение киберпреступности таково: «Использование киберпространства в незаконных целях с использованием уникальных функций киберпространства, таких как скорость и оперативность, удаленная работа, шифрование и запутывание, затрудняющих идентификацию операции и оператора».

Дискуссии о киберпреступности длятся уже не один год. Более десяти лет назад исследователи стали задаваться вопросом, что нового в киберпреступности, не является ли это просто старым явлением, использующим новые инструменты. Большинство исследователей представляют киберпреступность как уникальное явление [2, с. 77].

Когда проблема несет экзистенциальную угрозу (обычно для всего государства), она требует принятия чрезвычайных мер (тех, которые выходят за рамки обычных политических действий), затем она секьюритизируется.

В киберпространстве агентами угроз могут быть преступники, хакеры, террористы и государства в целом. Потенциальные жертвы, подверженные риску со стороны этих векторов угроз, также разнообразны. Субъекты угрозы могут заниматься кражей личных данных для совершения мошенничества, которое во взаимосвязанном мире киберпространства сделало бы всех людей в стране потенциальными жертвами.

В тех случаях, когда идентифицированной жертвой является государство и его институты, экзистенциальной угрозой ему может стать свержение режима. В случаях, когда отдельные граждане сталкиваются с риском для своего благосостояния (либо напрямую, либо в результате

потери государственных институтов), публичные действий могут быть оправданы, поскольку национальная оборона считается общественным благом. Поэтому политики должны быть заинтересованы в том, чтобы обезопасить отдельных граждан от таких угроз, ведь они обязаны защищать интересы своих избирателей.

В период пандемии произошел рост кибепреступлений. Их количество увеличилось в 1,5 раза. За семь месяцев 2021 года было зафиксировано 320 тысяч таких преступлений, рост составил 16%. На расследование кибепреступлений, как правило, уходят месяцы.

Для сравнения, в 2020 году количество киберпреступлений увеличилось на 94,6 %: в 2019 году их было зафиксировано 180 тысяч, а в 2016 году — 66 тысяч [3, с. 51].

21 июня 2021 года Министерство внутренних дел опубликовало статистику преступлений за январь–май 2021 года. Количество преступлений против личности снизилось, общее количество зарегистрированных преступлений увеличилось на 1,6% за счет цифровых преступлений.

Киберпреступность развивается и растет в ответ на пандемию COVID-19. Онлайн-мошенничество в Интернете нацелено на отдельных лиц, в то время как вымогательство в первую очередь подвергает риску системы, включая больницы [4, с. 42].

Правительствам и впредь будут угрожать вредоносные программы. Растущее распространение дезинформации будет продолжать сбивать с толку общественность.

Работа на дому привела к увеличению числа потенциальных жертв киберпреступности. Люди подвергаются повышенному риску в Интернете во время работы дома, что непреднамеренно увеличивает опасность для корпоративных ИТ-систем.

Будет по-прежнему развиваться фишинг, и мошенники будут стремиться получить доступ к критически важным системам, к конфиденциальным данным пользователей — логинам и паролям. Это значит, что в краткосрочной перспективе киберпреступность будет расти, и жертвы ее, скорее всего, столкнутся с тем, что раскрытия таких видов мошенничества им придется ждать долгое время.

Постоянная и разрушительная угроза кибератак, независимо от исполнителей, подрывает общую безопасность страны, поскольку по мере выявления основных уязвимостей киберпреступники используют их и переносят риски из области «кибер» в другие области, создавая своего рода системный беспорядок. От него органам национальной безопасности придется постоянно защищаться.

Заключение. По какому пути пойдет киберпреступность в ближайшие годы — важный вопрос, его сейчас активно обсуждают аналитики. Однако большинство их выводов основано на опыте разработок предыдущих лет, без учета текущих тенденций, из-за этого прогнозы отстают как минимум на 50%. Но даже если учесть все тенденции и тщательно их проанализировать, это не принесет уверенности в реализации всего запланированного в борьбе с таким видом мошенничества, потому что даже одно непредвиденное событие может радикально изменить все планы и наработки.

Убытки от киберпреступности в мире удвоились в период с 2015 по 2021 год — с трех до шести триллионов долларов. Наиболее популярными методами борьбы с киберугрозами во всем мире считаются антивирусная защита, клиентские межсетевые экраны, своевременная установка обновлений, резервное копирование данных, ограничение онлайн-активности, структурирование сети. Поскольку киберпреступность повсеместно не снижается, а продолжает расти, необходимо рассматривать ее в более широком контексте национальной и международной безопасности [5, с. 63]. Важно расширить понимание того, какие именно факторы могут способствовать национальной безопасности, и, следовательно, определить, какая конкретно защита необходима.

Библиографический список

1. Лебедь, В. Н. Управление процессами обеспечения кибербезопасности как фактор международной стабильности / В. Н. Лебедь, Б. И. Терещенко, К. А. Восканян // Коммуникология: электронный научный журнал. — 2017. — Т. 2. — № 4. — С. 30–37.

2. Попов, М. В. Кибербезопасность как элемент национальной безопасности России / М. В. Попов, Л. Н. Мамаева // Вестник Саратовского государственного социально-экономического университета. — 2019. — № 5 (79). — С. 80–82.

3. Номоконов, В. А. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология: вчера, сегодня, завтра. — 2012. — № 1 (24). — С. 45–55.

4. Киберпреступность как угроза национальной безопасности Российской Федерации / Р. Ж. Самиров, И. В. Примаков, С. Н. Синицын [и др.] // Законность и правопорядок в современном обществе. — 2014. — № 19. — С. 77–81.

5. Пилюгина, Т. В. Киберпреступность как угроза национальной безопасности в период пандемии: проблемы и меры предупреждения / Т. В. Пилюгина, А. А. Жуков // Право и практика. — 2020. — № 3. — С. 111–116.

Об авторах:

Мамцов Константин Геннадьевич, студент кафедры «Вычислительная техника и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), rexar1441@mail.ru

Ачилов Никита Рустамович, студент кафедры «Вычислительная техника и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), Nikitoosik.Achilov@mail.ru

About the Authors:

Mamtsov, Konstantin G., Student, Department of Computer Engineering and Information Security, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), rexar1441@mail.ru

Achilov, Nikita R., Student, Department of Computer Engineering and Information Security, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), Nikitoosik.Achilov@mail.ru