Сидорина Т.В., канд. экон. наук, доцент кафедры «Экономическая безопасность, учет и право» ФГБОУ ВО ДГТУ,
г. Ростов-на-Дону, Россия;
Sidorinatv@mail.ru
Тепегенджиян А.А., студент 5 курса ФГБОУ ВО ДГТУ,
г. Ростов-на-Дону, Россия;
angelina.tepenzi@gmail.com
Филев Д.В., студент 5 курса ФГБОУ ВО ДГТУ,
г. Ростов-на-Дону, Россия;
filiev94.25.99.z@gmail.com

КИБЕРПРЕСТУПНОСТЬ КАК ЧАСТЬ ТЕНЕВОЙ ЭКОНОМИКИ

Аннотация. В данной главе рассмотрена проблема киберпреступности, являющейся частью теневой экономики и ставшей специфическим бизнесом, а также являющейся угрозой экономической безопасности страны. Анализируются способы и методы борьбы с компьютерными преступлениями в современной России. Определены причины роста киберпреступлений, технологии, которые используются в данной сфере, позволяющие превратить кибермошенничество в бизнес.

Ключевые слова: киберпреступность, теневая экономика, экономический ущерб, экономическая безопасность.

Sidorina T.V., Cand. econom. Sci., Associate Professor of the Department of "Economic Security, Accounting and Law" FGBOU VO DSTU,
Rostov-on-Don, Russia;
Sidorinatv@mail.ru
Tepegendzhiyan A.A., 5th year student of FGBOU VO DSTU,
Rostov-on-Don, Russia;
angelina.tepenzi@gmail.com
Filev D.V., 5th year student of FGBOU VO DSTU,
Rostov-on-Don, Russia;
filiev94.25.99.z@gmail.com

CYBER CRIME AS A PART OF THE SHADOW ECONOMY

Annotation. This article examines the problem of cybercrime, which is part of the shadow economy and has become a specific business, as well as a threat to the country's economic security. The methods and methods of combating computer crimes in modern Russia are analyzed. The reasons for the growth of cybercrimes, the technologies that are used in this area, which make it possible to turn cyber fraud into a business, have been determined.

Key words: cybercrime, shadow economy, economic damage, economic security.

Обеспечение экономической безопасности РФ стало широкой проблемой не только с точки зрения распространенности, но и с точки зрения глубины и сложности угроз[2].

Актуальность темы обусловлена тем, что учитывая быстрые темпы развития киберпреступности, социальный риск и высокую скрытность, это явление становится все более распространенным и приобретает характер угрозы для всех.

Цель работы заключается в теоретическом анализе сущности киберпреступности, и какой ущерб, данная сфера теневой экономики, может понести за собой.

Первые компьютерные преступления связаны с банками: преступники изымали денежные средства со счетов клиентов. Изначально эти преступления были достаточно наивны, но угроза тем не менее получила все предпосылки к развитию. В нашей стране активно киберпреступность стала развиваться в конце девяностых.

В целом такие преступления называют мультимиллионным бизнесом, который, как и любой бизнес, ищет все новые возможности для развития и роста прибыли. Ориентировочная годовая «стоимость» киберпреступлений составляет 110 млрд долл. Ежегодно насчитывают около 556 млн жертв киберпреступности, более 1,5 млн в день. Популярность набирает и мошенничество с фейковыми объявлениями по продаже масок и антисептиков [7].

К основным криминологическим тенденциям в этой области относятся:

– общий рост числа экономических киберпреступлений на фоне некоторого снижения количества обычных экономических преступлений (всё больше мошенников выбирают Интернет как поле своей деятельности); увеличение общей суммы ущерба, нанесенного в результате таких преступлений;

– рост числа преступников-непрофессионалов (теперь для совершения компьютерных экономических преступлений не обязательно быть хакером и иметь специальные знания в области компьютерных технологий);

– смещение интересов мошенников в сторону частных лиц (раньше жертвами таких преступлений чаще становились банки и другие крупные организации, теперь ситуация изменилась, возможно, в результате массового использования частными лицами электронных платежей, электронных кошельков, онлайн-банков и других финансовых инструментов, реализуемых посредством компьютерных технологий)[1].

Прогнозируется, что к 2023 году масштаб киберпреступлений в России может вырасти с 14 до 30 процентов, если не будут выявлены новые эффективные технологии по борьбе с онлайн-правонарушениями [6].

До сих пор сотрудникам правоохранительных органов непросто найти злоумышленников, работающих в Интернете.

Приводя в пример статистические данные МВД России, можно сказать, что за последние 2 года удалось увеличить количество раскрытых ИТ-преступлений на два-три процента. Однако, за 9 месяцев 2019 года количество противоправных деяний, совершенных с использованием информационных технологий выросло на 70%, признаются в ведомстве, при этом уровень раскрываемости аналогичных преступлений остается невысоким – с 36% в 2016 году до 23% в 2019-м[5].

Говоря о проблемах выявления киберпреступности, следует отметить тот факт, что если данные правонарушения не будут решены в ближайшие годы, то,количество зарегистрированных уголовных дел в стране может увеличиться до 30–32% от общего числа регистрируемых уголовных дел в стране. Существующие базы данных, позволяющие анализировать большие объемы информации, включая личную, весьма неэффективны. «Planet», «Sherlock», «Osiris» и другие информационные базы, не гарантируют раскрытия киберпреступления. Для успешного раскрытия, информационные

серверы должны работать эффективно, что требует большой мощности компьютера и широкого круга обслуживающего персонала.

Главное, чтобы информация, собираемая мейнфреймерами, была связана с идентификаторами личной информации пользователя, а не с инструментами, используемыми преступниками. Сегодня преступники, использующие информационные технологии, используют инструменты, чтобы скрыть свою личность.

Также, стоит подчеркнуть тот факт, что любые катастрофы и чрезвычайные ситуации мошенники стараются использовать в своих целях. Сейчас злоумышленники стали распространять новости от имени Всемирной Организации Здравоохранения, призывая пользователей перейти по ссылкам для получения «секретной» информации о коронавирусе. Переходя по ссылке, пользователь незаметно для себя загружает вредоносное ПО, с помощью которого преступники в конечном счете получают доступ к счетам жертв. «Если ссылка в письме вас заинтересовала, наберите ее в браузере, а не переходите по ней», - предупреждает К. Игнатьев, руководитель группы анализа веб-контента «Лаборатории Касперского»[2].

Помимо широкомасштабных фишинговых атак, хакеры также могут проводить информационные атаки, сея панику и рассылая дезинформацию о распространении коронавируса. Кроме того, уже есть примеры диверсий в отношении учреждений, занятых борьбой с COVID-19. Так, хакеры уже смогли на продолжительное время обрушить серверы министерства здравоохранения и социальных служб США (HHS).

Кроме стандартных фишинговых писем угрозу предоставляют фейковые приложения. Например, под карты по распространению коронавируса маскируется зловредAZORuilt. Следует быть внимательными с диагностическими, информационными и любыми якобы имеющими отношение к пандемии приложениями.

Популярность набирает и мошенничество с фейковыми объявлениями по продаже масок и антисептиков. На сегодняшний день в российском

теневом интернете работают 73 сервиса, которые занимаются вербовкой инсайдеров в банках, ежедневно предоставляющих конфиденциальную информацию о клиентах[2].

Решить данную проблему маленького уровня раскрываемости киберпреступлений в стране возможно, если создать принципиально новую систему криминалистического учета и идентификации на основе электронно-цифровых следов различных сайтов. На сегодняшний день в России пока еще не поднимался вопрос об анализе электронно-цифрового следа централизованном сборе информации в криминалистических целях. В то же время, если возможно создать электронно-цифровой след совершенного преступления, это действительно эквивалентно установлению личности преступника.

Большинство нарушений информационных технологий – 80% - очень мелкие, ущерб от каждого составляет менее 5 тысяч рублей. Такие дела не подпадают под уголовное право. Кроме того, каждая пятая жертва подобной практики не сообщает об инциденте в полицию. Отметим, что в течение года совершается порядка 300 миллионов попыток атак, 99% из которых автоматически блокируются с помощью аппаратных и программных сервисов. Например, по словам компании «Россеть», специалисты компании каждый год отражают более девяти миллионов попыток хакерского проникновения по корпоративным параметрам. Однако за покушения также может быть установлена уголовная ответственность.

Исходя из вышесказанного, можно вполне обоснованно утверждать, что противодействие преступлениям, совершенных с помощью IT технологий, неразрывно связано с обеспечением экономической безопасности нашей страны.

Таким образом, но основе широкого спектра видов интернет-преступлений можно сделать вывод, что способы совершения преступлений интернет-преступников постоянно совершенствуются. Появляются все более изощренные методы, что в свою очередь постоянно заставляет

криминалистов находить новые способы выявления и пресечения подобных видов преступлений. Однако, специфика использования виртуального пространства, как места совершения преступления, создает условия анонимности личности преступника, даже не смотря на появляющиеся способы деанонизации пользователей сети[3].

Разумеется, что угроза информационному ресурсу государства – угроза национальной безопасности. Но, нормы и положения в этой сфере до сих пор четко не определены. Причиной для этого служит: развитие научно-технического прогресса создает благоприятные возможности для кражи денег с электронных систем взаиморасчетов, несанкционированного использования ЭВМ (для получения собственности или услуг), повреждения или уничтожения компьютерных сетей и программ, проникновение в чужие базы данных, незаконного копирования или фальсификации данных, шантажа, информблокады, шпионажа и т. д [4].

Кроме того, глобальное распространение информационно-коммуникативных технологий в обществе привело к появлению и развитию принципиально нового вида терроризма – информационного терроризма или кибертерроризма. Большое значение в этом контексте приобретает научно-методическое обеспечение деятельности правоохранительных органов РФ и странах Центральной Азии по определения теоретических, а также тактических аспектов противодействия информационному терроризму (кибертерроризму).

В современных реалиях доступа нашей страны в единое информационное пространство, необходимо системное и последовательное противодействие киберпреступности– как в целом, так и отдельно. Чтобы уменьшить ущерб, наносимый экономике, необходимо принять эффективные меры по борьбе с киберпреступностью и ее предотвращению, включая разработку законодательства, в том числе международного права в области информационной и кибербезопасности.

Библиография

1. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. –2019. – № 1. – С. 25-33. – URL:https://cyberleninka.ru/article/n/vidy-kiberprestupleniy-po-rossiyskomu-ugolovnomu-zakonodatelstvu/viewer

2. Кибермошенники включили новый вирус в свой арсенал.*[Электронный ресурс]*–URL:https://rg.ru/2020/03/17/kibermoshenniki-vkliuchili-novyj-virus-v-svoj-arsenal.html

3. Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. –2017.– № 3. –С. 162-169.– URL:https://cyberleninka.ru/article/n/opredelenie-ponyatiya-kiberprestuplenie-otdelnye-vidy-kiberprestupleniy/viewer

4. Русскевич Е.А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Международное уголовное право и международная юстиция. –2018. – № 3.– С. 10-13.–URL:https://urfac.ru/?p=416

5. Степанов О.А. Актуальные проблемы противодействия кибертерроризму: монография. М., 2014.–URL:https://search.rsl.ru/ru/record/01008133794

6. Черноусов И. Потери организаций от киберпреступности [Электронный ресурс] – URL:https://www.tadviser.ru/index.php/

7. Официальный сайт Министерства внутренних дел Российской Федерации *[Электронный ресурс]*–URL:https://мвд.рф/reports/item/22678184/

References

1. Ivanova L.V. Types of cybercrimes under Russian criminal law // Legal Research. - 2019. - No. 1. - P. 25-33. - URL: https: //cyberleninka.ru/article/n/vidy-kiberprestupleniy-po-rossiyskomu-ugolovnomu-zakonodatelstvu/viewer

2. Cyber fraudsters have included a new virus in their arsenal. [Electronic resource] - URL: https://rg.ru/2020/03/17/kibermoshenniki-vkliuchili-novyj-virus-v-svoj-arsenal.html

3. Kochkina E.L. Definition of the concept of "cybercrime". Certain types of cybercrimes // Siberian criminal procedural and criminalistic readings. - 2017. - No. 3. - S. 162-169. - URL: https: // cyberleninka.ru/article/n/opredelenie-ponyatiya-kiberprestuplenie-otdelnye-vidy-kiberprestupleniy/viewer

4. Russkevich E.A. International legal approaches to countering crimes committed using information and communication technologies // International criminal law and international justice. - 2018. - No. 3. - P. 10-13. - URL: https: // urfac.ru/?p=416

5. Stepanov O.A. Actual problems of countering cyber terrorism: monograph. M., 2014. - URL: https://search.rsl.ru / ru / record / 01008133794

6. Chernousov I. Losses of organizations from cybercrime [Electronic resource] - URL: https: //www.tadviser.ru/index.php/

7. Official website of the Ministry of Internal Affairs of the Russian Federation [Electronic resource] - URL: https: //mvd.rf/reports/item / 22678184 /