БАБАНИН Артемий Олегович
Финансовый университет при Правительстве Российской Федерации, Ленинградский проспект, д. 49, Москва, 125993, Россия.
https://orcid.org/0000-0002-2208-604X
Бабанин Артемий Олегович, студент 3 курса, факультет Международных экономических отношений (МЭО), Москва. E-mail: artem240899@mail.ru

Научный руководитель: Куприянова Людмила Михайловна – кандидат экономических наук, доцент, заместитель заведующего кафедрой «Экономика интеллектуальной собственности», доцент Департамента учета, анализа и аудита. E–mail: KuprianovaLM@yandex.ru
https://orcid.org/0000-0002-9453-6425
Финансовый университет при Правительстве Российской Федерации, Ленинградский проспект 49, Москва, 125993, Россия, Москва

КИБЕРПРЕСТУПНОСТЬ НА МИРОВЫХ ФИНАНСОВЫХ РЫНКАХ

Аннотация

В данной статье исследованы основные виды киберпреступлений, распространенные на мировых финансовых рынках. Изучение преступности в интернете крайне актуально в настоящее время, так как объемы краж конфиденциальной информации и денежных средств в этом секторе экономики растут из года в год. Кроме общей информации о каждом виде киберпреступления в статье прдставлены их отличительные характеристики и оценена опасность.

Для проведения данного исследования были собраны и проанализированы данные об атаках хакеров на систему безопасности населения таких стран как США, Англия и Россия, а также крупных международных компаний и выяснены размеры причиненного ущерба. Особое внимание уделено оценке опасности каждого вида киберпреступления; выделены основные цели атак преступных группировок, совершающих то или иное интернет – преступление, и защитная стратегия. В статье представлены данные, опубликованные Федеральной службой государственной статистики различных стран, сайты бизнес аналитики и правовые документы. Проведен анализ данных по теме исследования и предложены пути дальнейшего противостояния этому виду преступности с учетом опыта прошлых лет и прогнозов развития технологий.

Ключевые слова: *киберпреступность, интернет, государственное регулирование, финансы, кража*

JEL classification: K23

Artemii O. Babanin, 3nd year student, Faculty of International economic relations, Finance University under the Government of the Russian Federation, Moscow. E-mail: artem240899@mail.ru

Supervisor: Lyudmila M. Kupriyanova, Ph.D. in Economics, Associate professor, Deputy Head of the Department of Economics of Intellectual Property, Associate professor of the Department of Accounting, Analysis and Audit, Finance University under the Government of the Russian Federation, Moscow

CYBERCRIME ON THE GLOBAL FINANCIAL MARKETS

Abstract

In this article we will discuss the main types of cybercrime, common in the global financial markets today. The study of crime on the Internet is extremely important now, as the volume of thefts of confidential information and money in this sector of economy is growing from year to year. In addition to general information about each type of cybercrime, their distinctive characteristics and risk assessment will also be given.

To carry out this study, we will collect and analyze data on hacker attacks on the population of countries such as the United States, Great Britain and Russia, as well as large international companies and find out the size of the damage. Particular attention will be paid to the assessment of the danger of each type of cybercrime; we will highlight the main objectives of attacks by criminal groups that commit an Internet crime and try to develop a protective strategy. The data published by the Federal state statistics service of various countries, business Analytics websites and legal documents will be used in the course of writing the article. After studying all the necessary materials, we will conduct a detailed analysis and propose ways to further confront this type of crime, taking into account the experience of past years and forecasts of technology development.

Keywords: *cybercrime, Internet, government regulation, Finance, theft*

С начала 60-х годов XX века параллельно нашему миру начал свое существование еще один. Этот мир создали мы сами для получения новых возможностей и облегчения своей жизни. Однако было забыто, что созданное в мирных целях, тоже может нести угрозу.

В этой статье речь пойдет про основные угрозы финансовому благополучию людей и компаний, появляющиеся с цифровизацией экономики. Любая, даже самая безобидная вещь в руках злоумышленников может оказаться разрушительной, а когда под этой вещью подразумевается интернет, то проблемы борьбы с интернет-преступниками становятся глобальными.

Наиболее распространенные преступления, которые можно совершать, не покидая дом или офис и не прилагая почти никаких усилий - это кража данных и средств и взломы, которые становятся все более популярными в наши дни.

В экономике киберпреступления начались в 1990-х, когда в пластиковые банковские карты стали монтироваться электронные чипы и для их считывания были разработаны программы и базы данных, в которых хранилась вся информация о владельце карты, а также все его деньги, находящиеся на электронном счете. Именно тогда люди, не желавшие зарабатывать честно, решили с помощью хакерских программ взламывать электронные счета и присваивать деньги себе. С ходом времени эта сфера преступности развилась и глубоко внедрилась в банковскую сферу, принося все большие убытки компаниям и банкам.

Для того чтобы говорить о киберпреступности, рассмотрим сначала ее виды и выясним какую угрозу они представляют.

Наиболее популярным видом преступлений в финансовой сфере является кардерство. Это один из старейших видов финансовой киберпреступности представляющий собой кражу кредитных карт, а также нарушение электронных связей и средств зашиты, позволяющее злоумышленникам использовать чужие кредитные и дебетовые карты. Однако по прогнозам экспертов в области платежных систем, банковского дела и процессинга, к 2020 г. почти у двух третей населения развитых стран мира банковские карты заменит гаджет, из этого можно сделать вывод о том, что в ближайшие годы весь кардинг будет переходить в киберпространство. Без соответствующих блокировок программных решений безопасности, а также сложных программ, которые дают возможность преодолеть не только одноуровневую, но и многоуровневую систему идентификации, даже украденный телефон не будет иметь никакой пользы для преступника. В связи с этим есть все основания полагать, что в этой сфере появятся высокотехнологичные преступные группировки, которые смогут вытеснить или подчинить преступников-одиночек и неорганизованные группы, действующие на этом рынке в настоящее время. Если говорить об ущербе, нанесенном кардингом в мировом масштабе, то ориентировочно он составляет около 15—20 млрд. долларов в год.

Быстро развивающимся направлением киберпреступности является пеймент – криминал: использование преступниками процессинговых и иных платежных систем. Этот вид преступлений является наименее рискованным. Стоит отметить, что в истории правоохранительных органов различных государств были зафиксированы только 4 случая выявления с наказанием преступников, притом, что всего было обнаружено более 50 подобных случаев в этих государствах. Отличием его от кардерства является то, что пеймент-преступниками не осуществляется прямая кража средств с дебетового или кредитного счета физических и юридических лиц. Указанный вид преступности основан на высоком уровне программирования и хакинге. Преступниками взламываются коды коммуникаций процессинговых центров и платежных систем и добавляется к каждому выбранному или полученному на основе генератора случайных чисел платежу некоторая, как правило, незначительная дополнительная сумма. В соответствии с исследованиями американских и британских специалистов в сфере финансовой кибербезопасности в США менее 5%, а в Британии — менее 7% клиентов обращают внимание на добавленную сумму, когда она составляет не больше 1 % от общей суммы платежа. Клиенты, зачастую, считали, что данная сумма выступает неким дополнительным тарифом платежной или процессинговой компании, который взимается по той или иной причине. На первый взгляд прибыль крайне мала при внушительных первоначальных затратах, необходимых

для оснащения аппаратами, найма хакеров и программистов, тем не менее, потенциальная прибыль исчисляется миллионами. Так, ежедневно в Великобритании население, а также малый и средний бизнес при помощи систем электронных платежей и независимых платежных систем переводят средства, равные нескольким десяткам миллиардов фунтов стерлингов.

Сегодня цифровые активы банков и других финансовых институтов, включая корпоративно-информационные системы, аппаратную часть, базы данных, клиентские, торговые, учетные и иные программы, своей стоимостью составляют более 70 % неденежных активов всего финансового сектора. Именно поэтому в настоящее время популяризируется криминальное программирование. Целостное и сохранное состояние цифровых активов банков выступает залогом их эффективной работы и конкурентоспособности. От качества, конфиденциальности и защищенности программного обеспечения, внедряемого ИКТ в банковский сектор, зависит как благосостояние финансовых институтов, так и уже упомянутая конкурентоспособность.

Программные продукты становятся основными производственными факторами, в этой связи, у данного сектора с мультипликативным эффектом возрастают размеры ущерба, который может быть нанесен разработчиками и системными администраторами, занимающимися созданием, обслуживанием и совершенствованием указанных финансовых продуктов. Выделяют два основных фактора, способствующих резкому росту издержек финансовых институтов, и как следствие и доходов преступных группировок от деятельности отдельных криминальных финансовых программистов.

Первый связан с тем, что будет продолжаться экспансия ИКТ-технологий в финансовый сектор. Достоверно известно, что уже к 2020 г. этот сектор превратится в один из наиболее автоматизированных секторов экономики. Второй характеризуется тем, что это будет происходить во время того, как выпускники ведущих университетов будут выбирать такие перспективные направления, как синтетическая биология, биоинформатика, глубокое машинное обучение и искусственный интеллект вместо традиционного программирования. В таких условиях компании, работающие в сфере финансового программирования, а также банки и иные финансовые институты столкнуться с необходимостью нанимать программистов и разработчиков из стран третьего мира. Не секрет, что в большинстве этих стран ослаблена деловая этика в силу ряда исторических причин, а также не сформировано уважение к закону. Совокупность отмеченных выше двух факторов заставляет пессимистично смотреть на развитие финансового сектора в ближайшем будущем, а также на возможность сократить потери и убытки от криминального программирования. Скорее всего, они будут только возрастать.

Крайне трудно бороться с процессом или явлением, которые не диагностированы и не оценены, а отсутствие количественной оценки размеров ущерба от преступности мешает эффективной борьбе с ней. Только при наличии общедоступной статистики, можно стремиться к минимизации размеров ущерба от криминального программирования для финансового сектора.

Программный инжиниринг - еще один известный вид IT-преступлений, представляющий собой сочетание хакерства со злонамеренным внесением в программный код покупных или собственных программ, ответственных за хранение, учет, обработку данных, и принятие на их основе финансовых и инвестиционных решений. С начала 21 века международная банковская система все быстрее переходит на электронное хранение данных, электронные деньги, и электронный документооборот. Именно он становится общеделовым стандартом, присущим финансовым институтам технологически развитых стран. Вместе с переводом отчетности, бухгалтерских, платежных и юридических документов в электронную форму преступная деятельность во многом стала легче.

В традиционных финансах и экономике с бумажным документооборотом и персональным общением всех участников финансовых и бизнес-процессов было трудно без сознательного содействия участников подменить платежные документы и данные бухгалтерской отчетности. С появившимися изменениями, а также с заменой живого общения использованием мессенджеров, коммуникаторов и электронной почты возможности киберпреступников значительно возросли. Получая доступ к скрытой информации компании или банку за счет использования методов социального инжиниринга, киберпреступные группировки получают возможность не разрушать, а подменять различного рода данные. При этом в большинстве случаев замену данных оказывается невозможно отследить и обнаруживается она лишь после осуществления крупных мошеннических платежей.

Согласно мнению сотрудников правоохранительных органов, использование методов социального инжиниринга дает возможность вовлечения в криминальную деятельность сотрудников банков и других финансовых учреждений таким образом, что они даже не подозревают об этом, полагая, что просто выполняют указания вышестоящих уровней управления или собственников.

В современных реалиях жертвой преступлений, совершаемых в виртуальном пространстве, может стать любой пользователь. Жертвы могут быть простыми гражданами и организациями, так и государственными органами или даже государствами. Масштабы ущерба от киберпреступлений преступлений имеют весьма высокие показатели. Совокупный ущерб от киберпреступлений, согласно ежегодному докладу Центра по борьбе с преступлениями в сети Интернет (ICCC), в России в

2017 г. достиг уровня 233 млрд. рублей, а средний ущерб в расчете на одно преступление составил 5,63 млрд. рублей.

Согласно статистике, представленной на сайте PWC, около 70% россиян хотя бы раз в своей жизни подвергались хакерским атакам. Можно сделать вывод, что от деятельности киберпреступников страдает абсолютно все население, использующее электронные гаджеты. В среднем, каждый месяц в России успешно атакуют 1-2 банка: средний ущерб от атаки — 132 млн. руб (2 млн. долл.). Эксперты Group-IB констатируют, что количество целенаправленных атак на банки с целью хищения через SWIFT за отчетный период увеличилось в три раза. Снижение угроз со стороны банковских вирусов для ПК в России продолжается с 2012 года. Атаки на физических лиц ушли в прошлое, а ущерб для юридических лиц по итогам отчетного периода сократился еще на 12% и составил 547 800 000 рублей (8,3 млн. долл.).

Рынок платформенных вирусов после нескольких лет роста остановился в России, но продолжает развиваться на мировой арене. Количество проводимых ежедневных хищений с их помощью в России снизилось почти в три раза. Также стоит отметить сокращение среднего размера хищений с 11 тысяч рублей 2017 году, до 7 тысяч в 2018. Веб-фишинг по-прежнему продолжает терроризировать весь мир. Количество групп, которые создающих фишинговые сайты под российские бренды выросло с 15 до 26. В России общее количество успешных фишинговых атак, совершаемых ежедневно, выросло до 1274 (ранее — 950), было похищено 251 млн. рублей, что на 6% больше, относительно 2017 года.

На международном рынке, в отличие от прошлого периода, первую позицию заняли фишеры, нацеленные на облачные хранилища, а не на финансовый сектор. По объему фишинговых сайтов в мире США занимает 1 место (80%), 2 место — Франция, 3-е — Германия. Согласно отчету Group-IB, 73% всех фишинговых ресурсов попадают в следующие три категории: облачные хранилища (28%), финансовые (26%), и онлайн-сервисы (19%)

Осознание того, что справиться с новыми криминальными угрозами возможно только совместными усилиями всех государств приходит с пониманием масштабов киберпреступности, которые продолжают расширяться из-за новых коммуникационных технологий. В современных условиях наметилась тенденция к унификации законодательства и координации правоохранительной деятельности в мировых масштабах. В уголовном законодательстве нашей страны ключевой проблемой является категориально-понятийный аппарат, который используется для описания киберпреступлений. Нельзя отрицать, что наличие основных понятий в тексте законодательства, характеризующего данные преступления, является важным и необходимым.

В главе 28 Уголовного кодекса Российской Федерации приведены уголовно наказуемые деяния в сфере компьютерной информации, при этом

ни в самом уголовном кодексе, ни в различных комментариях к нему, не получили широкого отражения применение электронных информационно-коммуникационных способов и средств сбора, накопления и распространения электронной информации. Применение DDoS-атак, скимминга, фишинга, а также другие средства и способы совершения киберпреступлений также не нашли конкретное отражение в Уголовном кодексе.

На данный момент и законодательство, и силовые структуры находятся на стадии активной модернизации и готовности дать отпор преступникам, действующим через интернет. Безусловно, есть и продвижения в области противодействия интернет – преступлениям. Например, в рядах МВД РФ был сформирован первый отдел по борьбе с преступностью в интернете, который уже добился некоторых успехов. В связи с прогнозом на активное развитие киберпреступности многие банки и крупные корпорации выделяют большие суммы денег на разработку и усиление систем безопасности, которые позволят сдержать или предотвратить хакерские атаки на их расчетные счета. По данным Росстата за 2018 год, 22,9% от общей суммы финансирования исследовательской деятельности из бюджета РФ идут именно на создание новых способов защиты государственных и частных сбережений. Безусловно, исследования в области обеспечения цифровой экономической безопасности будут вестись еще не один десяток лет, и противостояние между преступниками и их жертвами усилиться, но при условии соблюдения предосторожности, снизить ущерб от деятельности хакеров и обезопасить свои счета и сбережения станет легче.

Таким образом, киберпреступления оказывают влияние на финансовые секторы всех стран, включая Россию, ущерб от них может исчисляться миллиардами долларов и пострадать от деятельности хакеров могут как крупные компании, так и обычные люди. К счастью, противодействие киберпреступлениям находится сейчас на стадии активного развития, создаются особые отделы по борьбе с интернет-преступниками, обновляются нормативно-правовые документы, меняется в этом направлении законодательство и ужесточаются наказания на преступления в интернете. И, возможно, вскоре будут найдены эффективные методы борьбы и придуманы меры наказания для представителей данного сектора преступности.

Список источников:

1. Кодекс об административных правонарушениях Российской Федерации
2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ
3. Черных А.В. Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) // Советское государство и право. 1990. N 6. С. 31 - 38.

4. Уголовное право. Особенная часть: Учебник для вузов / Под ред. Н.И. Ветрова, Ю. И. Ляпунова. М., 1998. С. 768.

5. Сайт компании Group-IB [Электронный ресурс]: Кибертерроризм в России - Режим доступа: http://www.group-ib.ru/media/tag/cyberterrorism/ 16.02.2019

6. Сайт компании PWC – [Электронный ресурс]: Российский обзор экономических преступлений - Режим доступа: http://www.pwc.ru/ru/ceo-survey 16.02.2019

7. Сайт компании Microsoft - [Электронный ресурс]: Обзор мировых киберпреступлений - Режим доступа: https://www.microsoft.com/en-us/research/publication/sex-lies-and-cyber-crime-surveys/

8. Консультант плюс – сайт правовой поддержки [Электронный ресурс]: Киберпреступления - Режим доступа http://www.consultant.ru/search 18.02.2019

9. Tadviser – сайт бизнес-аналитики [Электронный ресурс]: Киберпреступность в России и ее влияние на экономику страны– Режим доступа: http://www.tadviser.ru 19.02.2019

10. Молодой ученый – научный журнал [Электронный ресурс]: Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия – Режим доступа: https://moluch.ru/archive/133/37306/ 19.02.2019

11. FloridaTech – сайт Технологического института штата Флорида [Электронный ресурс]: A brief history of cyber crime – Режим доступа: https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/ 19.02.2019

12. Сайт федеральной службы по финансовому мониторингу [Электронный ресурс] – Потери от преступлений в финансовом секторе – Режим доступа: http://www.fedsfm.ru/ 19.02.2019

13. Федеральная служба государственной статистики сайт [Электронный ресурс - Эффективность экономики России – Режим доступа: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/efficiency/ 19.02.2019

References:

Code of administrative offences of the Russian Federation

Criminal code of the Russian Federation of 13.06.1996 N 63-FZ

Chernykh A.V. Ensuring the security of automated information systems (criminal law aspects) // the Soviet state and law. 1990. N 6. P. 31 - 38.

The website of the company Group-IB [Electronic resource]: Cyber-terrorism in Russia - the Regime of access: http://www.group-ib.ru/media/tag/cyberterrorism/ 16.02.2019

Criminal law. Special part: Textbook for universities / Ed.So. Vetrova, Yu. I. Lyapunov. M., 1998. P. 768.

Company website PWC [Electronic resource]: the Russian economic crime survey - Mode of access: http://www.pwc.ru/ru/ceo-survey 16.02.2019

The Microsoft website - [Electronic resource]: a Review of the global cybercrime - available at: https://www.microsoft.com/en-us/research/publication/sex-lies-and-cyber-crime-surveys/

Consultant plus – legal support site [Electronic resource]: Cybercrime - access Mode http://www.consultant.ru/search 18.02.2009

Tadviser – business intelligence website [Electronic resource]: Cybercrime in Russia and its impact on the country's economy– access Mode: http://www.tadviser.ru 19.02.2009

Young scientist – scientific journal [Electronic resource]: cyber crime: issues of criminal-legal assessment and organization of counter – Regime of access: https://moluch.ru/archive/133/37306/ 19.02.2019

FloridaTech website of Technological Institute of Florida [Electronic resource]: A brief history of cyber crime – Mode of access: https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/ 19.02.2019

Website of the Federal service for financial monitoring [Electronic resource] – Losses from crimes in the financial sector – access Mode: http://www.fedsfm.ru/ 19.02.2009

Federal state statistics service website [Electronic resource - Efficiency of the Russian economy – Access mode: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/efficiency/ 19.02.2009