Александра Владимировна Тарханова
студентка направления «Юриспруденция» Тюменского государственного университета, г. Тюмень a.v.tarkhanova@mail.ru
Рината Ринатовна Гарипова
студентка направления «Юриспруденция» Тюменского государственного университета, г. Тюмень, garipova.rinata@inbox.ru
Елена Александровна Тарханова
кандидат экономических наук, доцент кафедры экономики и финансов Тюменского государственного университета, г. Тюмень, tarhanova333@mail.ru

КИБЕРПРЕСТУПЛЕНИЯ В ФИНАНСОВОЙ СФЕРЕ: ОЦЕНКА ТЕКУЩЕЙ СИТУАЦИИ В РОССИИ

Аннотация. Финансовый сектор России является объектом повышенного внимания со стороны злоумышленников, так как концентрирует в себе огромные финансовые ресурсы. Киберпреступность является одной из ключевых проблем финансовой сферы. Активное развитие цифровизации финансового рынка способствовало усилению интереса мошенников, которые трансформировались под требования новой цифровой среды. В рамках данной статьи проведена оценка текущей ситуации с киберпреступностью в финансовой сфере России, представлена динамика кибератак на финансовые организации и предложен ряд мер по борьбе с кибермошенниками.
Ключевые слова: финансовая сфера, киберпреступления, кибератаки, кибермошенничество.

Aleksandra Vladimirovna Tarkhanova
Student of the specialty "Jurisprudence" at University of Tyumen, Tyumen, a.v.tarkhanova@mail.ru
Rinata Rinatovna Garipova
Student of the specialty "Jurisprudence" at University of Tyumen, Tyumen, garipova.rinata@inbox.ru
Elena Aleksandrovna Tarkhanova
Candidate of Economics, Associate Professor of the Department of Economics and Finance at University of Tyumen, Tyumen, tarhanova333@mail.ru

CYBERCRIMES IN THE FINANCIAL SPHERE: ASSESSMENT OF THE CURRENT SITUATION IN RUSSIA

Abstract. The financial sector of Russia is the object of increased attention from intruders, as it concentrates huge financial resources. Cybercrime is one of the key problems of the Russian financial sector. The active development of the digitalization of the Russian economy contributed to the increased interest of fraudsters, who transformed themselves to the requirements of the new digital environment. Within the framework of this article, an assessment of the current situation with cybercrime in the financial sector of Russia is carried out, the dynamics of cyber attacks on financial organizations is presented and several measures to combat cybercriminals are proposed.
Keywords: financial sphere, cybercrime, cyberattacks, cyber fraud.

В России финансовый сектор является одним из наиболее заинтересованных в обеспечении достаточного уровня защищенности [1]. На постоянной основе происходит совершенствование нормативно-правовой базы и поддержка непрерывного информационного обмена между Автоматизированной системой обработки инцидентов (АСОИ ФинЦЕРТ) и финансовыми организациями.

Любое изменение в финансовой сфере влияет на экономические показатели страны. Поэтому появление новых возможностей и внедрение новых технологий оказывают влияние не только на цифровизацию финансовой деятельности, но и на возникновение и развитие такого явления как кибермошенничество. Динамичное совершенствование финансовой сферы, в том числе, банковской сферы породило не только расширение различных цифровых продуктов и услуг, но и активное распространение кибермошенничества, возникновение которого связано как с появлением новых способов кражи данных и средств, так и с низким уровнем цифровой грамотности населения.

На протяжении всех этапов исторического развития России финансовая сфера представляла собой объект повышенного внимания мошенников [2]. В этой связи, говоря об активной цифровизации банковской системы и финансового сектора, можно утверждать, что интерес мошенников только усилился. Они трансформировались в кибермошенников, которые обучились новым способам кражи денег и данных клиентов.

Сегодня основными типами угроз для финансового, в том числе банковского, секторов являются: целевые атаки с целью получения доступа в корпоративную сеть для дальнейшей продажи или использования; программы-шифровальщики, способные привести к потере данных и остановке процессов; хищение денег у клиентов с использованием вредоносных программ и социальной инженерии; отмывание денег и финансирование терроризма; неправомерное использование бренда компании; шпионаж, кража и публикация информации, например о VIP-клиентах, их транзакциях и т. п. [3].

Анализ числа киберпреступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в России за период 2018-2022 гг., свидетельствует об их неуклонном росте (см. рис. 1). Данная тенденция фиксируется, несмотря на наличие в Уголовном кодексе РФ главы 28, предусматривающей уголовную ответственность за совершение киберпреступлений [4]. Преступления, совершаемые в данной сфере, чаще всего относят к ст. 159.6 «Мошенничество в сфере компьютерной информации».

В январе-феврале 2023 г. зарегистрировано 93,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 17,1% больше, чем за аналогичный период 2022 г. Это позволяет сделать вывод о том, что несмотря на активную антимошенническую политику, реальных результатов она не дает.

В целом, в сфере киберпреступлений сегодня отмечаются следующие тенденции:

1) с каждым годом наблюдается неуклонное увеличение количества преступлений, которое ничем не сдерживается;

2) в условиях цифровизации (в период 2019–2020 гг.) произошел резкий скачок совершаемых преступлений, что связано с пандемией COVID-19 и локдауном, вследствие чего людям приходилось пользоваться услугами в интернете;

3) наиболее «популярным» методом кибератак является социальная инженерия — звонки с незнакомых номеров, письма, приходящие на электронную почту или вирусные SMS.

Рис. 1. Динамика количества киберпреступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в России за период 2018-2022 гг.

Источник: составлено авторами на основе данных [5].

Ежегодно увеличивается количество кибератак, совершаемых на территории России, на различные организации, в том числе финансовый сектор. При этом за период 2018-2022 гг. наблюдается снижение доли кибератак на финансовый сектор (рис. 2).

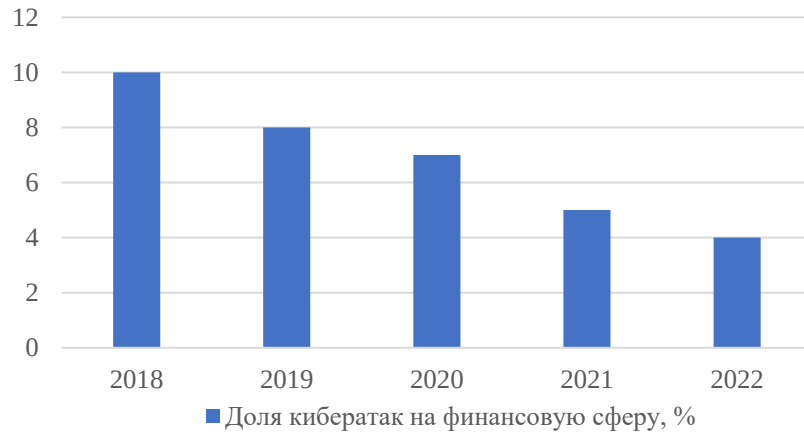

Рис. 2. Изменение доли кибератак на финансовый сектор в общем объеме кибератак на организации в России за период 2018-2022 гг., %

Источник: составлено авторами на основе данных [6-10].

Сегодня финансовый сектор характеризуется достаточно высокой подготовленностью к кибератакам мошенников. Однако уровень защиты данной сферы не является в полной мере достаточным. Итоги 2022 г. показывают сни-

жение кибератак на финансовые и банковские организации на 7%. По состоянию на 1 января 2023 г. доля атак на финансовый сектор составила около 4% от числа всех атак на организации (рис. 3).

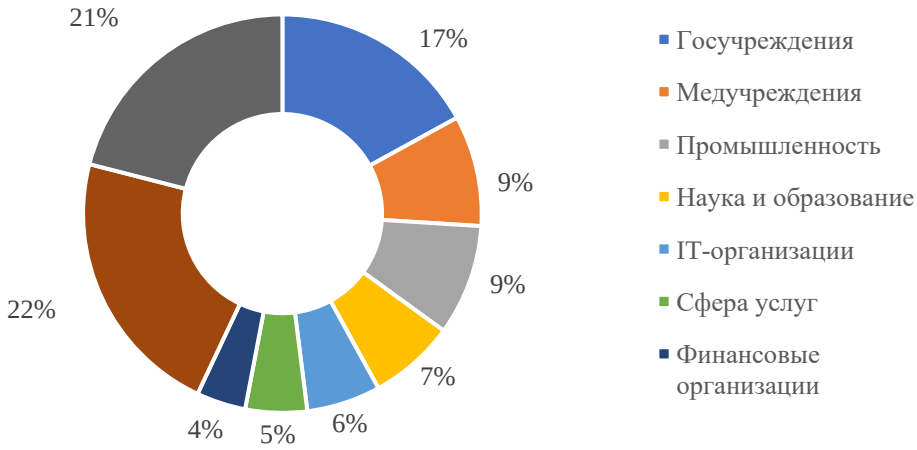

Рис. 3. Структура кибератак в разрезе отраслей экономики в 2022 г., %

Источник: составлено авторами на основе данных [9].

Нельзя не отметить, что главной целью мошенников, совершающих киберпреступления в финансовой сфере, является не столько похищение средств, сколько получение данных, то есть персональных данных клиентов, либо данных финансовой организации, которые содержат коммерческую тайну.

С целью предотвращения последствий и минимизации возникающих угроз необходимо гармонизировать нормативно-правовую базу в области регулирования финансовых технологий и безопасности субъектов экономики, особенно в части кибербезопасности и сохранности данных, а также акцентировать внимание на разработке финансовыми организациями собственной политики безопасности. Важным также является и повышение цифровой грамотности населения. В 2022 г. уровень цифровой грамотности в России повысился по сравнению с 2018 годом и составил 71%.

Действия злоумышленников могут привести к реализации недопустимых для финансовой сферы событий, и поэтому прежде всего необходимо оценить, какие бизнес-процессы зависят от работоспособности веб-приложений и как атака на веб-ресурсы может повлиять на деятельность организации и ее клиентов. Необходимо регулярно проводить анализ защищенности приложений и обновлять программное обеспечение в соответствии с сообщениями вендоров, использовать межсетевой экран уровня приложений, внедрять процесс безопасной разработки веб-приложений [1].

В целом, защищенность финансовых организаций с каждым годом повышается. Для проведения атаки и извлечения финансовой выгоды злоумышлен-

нику нужны более высокая квалификация и глубокие знания внутренних бизнес-процессов, чем при взломе компаний других отраслей, поэтому интенсивность атак на финансовые организации постепенно снижается, а основным орудием преступников становится социальная инженерия [1]. В то же время увеличивается активность киберпреступников по торговле доступами в корпоративную сеть банков и поиску нелояльных сотрудников. Результаты тестирований на проникновение и верификации недопустимых событий показывают, что, несмотря на относительно хороший уровень защиты от внешнего злоумышленника, финансовые компании могут понести серьезный ущерб от кибератаки. Поэтому они должны уделять особое внимание как регулярному тестированию на проникновение, так и верификации тех событий, которые могут повлечь серьезный ущерб и недопустимы для их деятельности [1].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Защищенность финансовой отрасли — промежуточные итоги 2022 г. // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-interim-2022/ (дата обращения: 13.04.2023).
2. Тарханова Е.А. Кибермошенничество как ключевая угроза процесса цифровизации банковской деятельности / Е А. Тарханова, А.В. Фрицлер // Экономическая безопасность страны, регионов, организаций различных видов деятельности: Материалы Третьего Всероссийского форума в Тюмени по экономической безопасности, Тюмень, 20–21 апреля 2022 г. / отв. редактор Д.Л. Скипин. — Тюмень: ТюмГУ-Press, 2022. — С. 303-306.
3. Батюкова В. Е. Состояние киберпреступности в банковской сфере / В.Е. Батюкова // Государственная служба и кадры. 2021. № 3. — URL: https://cyberleninka.ru/article/n/sostoyanie-kiberprestupnosti-v-bankovskoy-sfere (дата обращения: 13.04.2023).
4. Уголовный кодекс РФ // КонсультантПлюс: надежная правовая поддержка: сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 13.04.2023).
5. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2022 г. // Министерство внутренних дел РФ: сайт. — URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 13.04.2023).
6. Актуальные киберугрозы: итоги 2019 г. // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/ (дата обращения: 13.04.2023).
7. Актуальные киберугрозы: итоги 2020 г. // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения: 13.04.2023).
8. Актуальные киберугрозы: итоги 2021 г. // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения: 13.04.2023).
9. Актуальные киберугрозы: итоги 2022 г. // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 13.04.2023).
10. Защищенность кредитно-финансовой сферы, итоги 2018 г. Оценка Positive Technologies // Positive Technologies: сайт. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/credit-and-financial-security-2019/ (дата обращения: 13.04.2023).