Киберпреступность как угроза экономической безопасности банковской сферы

Cybercrime as a Threat to the Economic Security of the Banking Sector

(DOI: 10.34773/EU.2021.5.19)

Л. КУРМАНОВА, А. ГАЛИМАРДАНОВ

Курманова Лилия Рашидовна, д-р экон. наук, профессор кафедры финансов и налогообложения Института экономики, финансов и бизнеса Башкирского государственного университета (ИНЭФБ БашГУ). E-mail: kurmanova_ugaes@mail.ru

Галимарданов Артур Рамилович, аспирант кафедры финансов и налогообложения ИНЭФБ БашГУ. E-mail: galimardanov.a@yandex.ru

В статье рассматриваются вопросы, связанные с экономической безопасностью в банковской системе России на основе исследования наиболее актуальных киберугроз, негативно влияющих на развитие банковского сектора и национальной экономики в целом. Анализируется ущерб от мошеннических действий и несанкционированных операций, связанных с киберпреступностью при предоставлении банковских услуг на основе онлайн-сервисов различным категориям клиентов, причем частота киберугроз характеризуется тенденцией к росту.

***Ключевые слова**: FinCERT, кибербезопасность, киберпреступность, мошенничество, финансовые организации, фишинг, вредоносные компьютерные программы.*

The article deals with issues related to economic security in the Russian banking system based on the study of the most urgent cyber threats that negatively affect the development of the banking sector and the national economy as a whole. The damage caused by fraudulent actions and unauthorized operations related to cybercrime in the provision of online banking services to various categories of customers is analyzed, and the frequency of cyber threats is characterized by an increasing trend.

***Key words**: FinCERT, cybersecurity, cybercrime, fraud, financial institutions, phishing, malicious computer programs.*

Введение

Внедрение современных информационных технологий и инноваций, направленных на улучшение жизни человечества, а также процессы глобализации и интеграции несут с собой и развитие новых методов мошенничества. Киберпреступность, как один из ключевых современных видов мошенничества, уже превратилась в глобальную международную проблему [1]. Обеспечение кибербезопасности является актуальной задачей современности, требует совершенствования инструментов выявления и устранения последствий киберрисков при предоставлении финансовых услуг и усиления информационной безопасности.

Мировой рынок кибербезопасности за последние пять лет вырос в 1,65 раза и составляет 202,3 млрд. долл. По прогнозам экспертов, к 2026 г. его объем достигнет порядка 352,4 млрд. долл. при среднегодовом темпе роста в 14,5 % [2]. Уровень готовности российских банков к переходу на цифровые технологии с позиции информационной безопасности составляет 64 %, что недостаточно и требует целенаправленных действий банковского сектора в управлении рисками и предотвращении возможных угроз [3].

С 2018 г. происходит рост интереса хакеров к криптобиржам, восемь из которых после атаки утратили ресурсы. В частности, повторная атака биржи YouBit (бывшая Yapizon) привела к потере 17 % ее активов и банкротству.

В последнее время наблюдается рост количества преступлений, квалифицируемых как «мошенничество с электронными средствами платежа», предусмотренных статьей 159.3 УК РФ, что связано с развитием информационных систем и использованием сети Интернет в предоставлении финансовых услуг. Участились компьютерные атаки в кредитно-финансовой

сфере. Данные преступления квалифицируются ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), ст. 273 («Создание, использование и распространение вредоносных компьютерных программ»), ст. 274 («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей») и ст. 274.1 («Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации») [7].

Методы исследования

Рассмотрение вопросов информационной безопасности банков в условиях развития цифровых сервисов осуществлялось на основе методологии статистических исследований в банковском секторе. Анализировались показатели, отражающие цифровую трансформацию финансовых услуг, поведение и приоритеты потребителей, риски финансовых технологий и др. Статистические методы в сфере финансовых услуг учитывают особенности социально-экономического и технологического характера протекающих в нем воспроизводственных процессов. Использование статистического аппарата при аналитических исследованиях позволило выявить процессы, протекающие в банковском секторе экономики, и тенденции их развития.

Результаты и обсуждения

Глобальное перемещение финансового сектора в сеть Интернет с помощью финансовых технологий инициировало серьезную проблему, связанную с обеспечением информационной безопасности, что привело к созданию в 2015 г. Центральным Банком Российской Федерации Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT Банка России). По данным Банка России, к информационному обмену FinCERT (ФинЦЕРТ) подключено 818 организаций, которые представлены не только кредитно-финансовыми организациями, но также компаниями-интеграторами, разработчиками антивирусного программного обеспечения, группами реагирования на инциденты, провайдерами и операторами связи, государственными органами власти и иными организациями (рис. 1).

Рис. 1. Участники информационного обмена, ед.
** Составлено с использованием источника [5]*

ФинЦЕРТ отслеживает мошеннические действия, связанные со счетами юридических лиц, платежными картами и незаконными операциями с банкоматами и терминалами. В 2020 г. количество несанкционированных списаний денежных средств со счетов компаний составило 293,3 тыс., что на 36 % меньше, чем годом ранее. Однако объем таких операций за 2020 г. существенно увеличился – с 701 млн рублей до 1020 млн рублей (рис. 2).

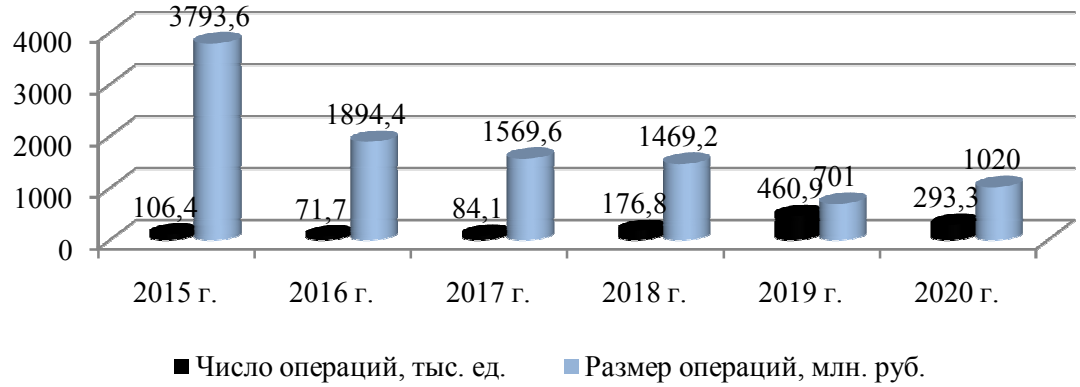

Рис. 2. Несанкционированное списание со счетов юридических лиц
** Составлено с использованием источника [5]*

Данные на рисунке 3 отражают динамику несанкционированного списания с платежных банковских карт. В 2020 г. количество попыток хищения денежных средств со счетов населения увеличились до 770,1 тыс. Объем таких операций за 2020 г. сократился до 2087,3 млн руб. Однако остается актуальным вопрос о необходимости расширения действий службы безопасности кредитных организаций применительно к исследуемому направлению и организации мер по пресечению инцидентов с киберпреступностью.

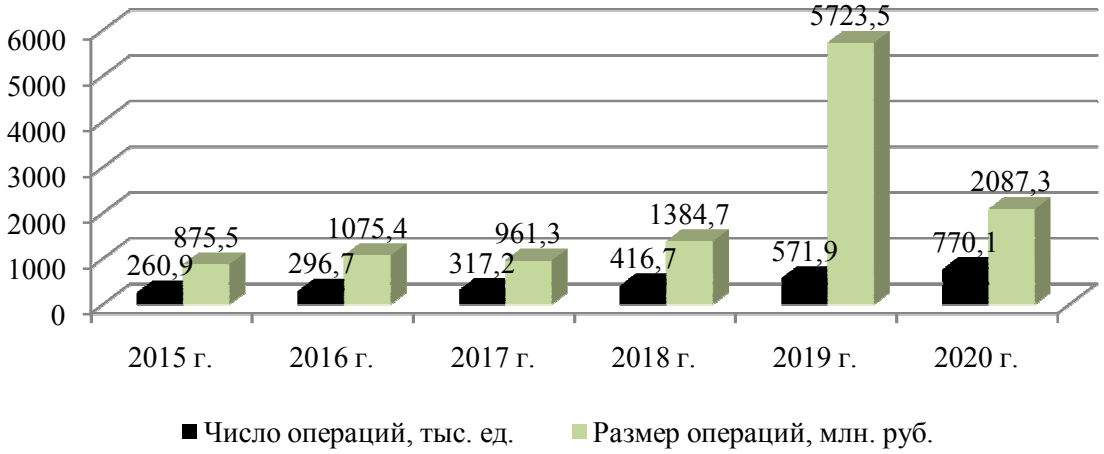

Рис. 3. Несанкционированное списание со счетов физических лиц
** Составлено с использованием источника [5]*

В результате информационного обмена при участии Автоматизированной системы обработки инцидентов (АСОИ ФинЦЕРТ) в 2020 г. было получено 968 сообщений о фактах распространения вредоносного программного обеспечения (ВПО), содержавших 1300 образцов ВПО. Анализ структуры объема ВПО позволяет отметить, что в 2020 г. доля шпионского ПО выросла более чем в 2,5 раза, и составила 58 %. Примерно 13 % занимает финансовое ВПО (рис. 4). ФинЦЕРТ Банка России зафиксировал 375 кампаний по распространению ВПО, из которых 71 была нацелена на кредитно-финансовые организации и их клиентов. По оценке экспертов, кибератаки привели к потерям в экономике России в размере 2,5 трлн. руб.

Широко распространенными формами атаки на счета являются использование методов социальной инженерии, фишинговые рассылки среди клиентов банков, использование вредоносного программного обеспечения, атаки, эксплуатирующие уязвимости программного обеспечения и др. [4].

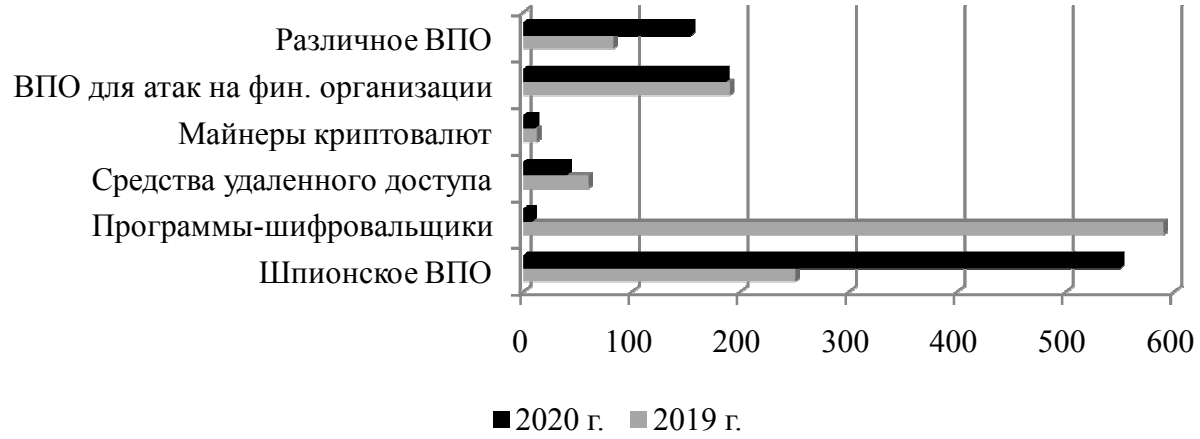

Рис. 4. Распределение ВПО по классам, ед.
** Составлено с использованием источника [5]*

Подчеркивается частота использования в качестве канала воздействия на предполагаемую телефонную связь (84 % случаев). Получение гражданами сообщений в различных мессенджерах, а также мошеннических смс-уведомлений составляет порядка 16 % случаев.

Данные таблицы свидетельствуют о росте мошеннического использования телефонных номеров по всем каналам (в 2–3 раза). Порядка 80 % звонивших злоумышленников выступали от лица представителей финансовых организаций, используя технологии подмены телефонных номеров. Основная категория граждан, подпадающих под мошеннические действия, является экономически активным населением в возрасте 20–60 лет. Чаще всего жертвами мошенников становятся женщины (более 65 %).

Количество мошеннических телефонных номеров, ед.

Показатели	2019 г., квартал				2020 г., квартал			
	I	II	III	IV	I	II	III	IV
Городские номера	223	1152	4365	5092	3473	3663	7641	4055
Мобильные номера	354	756	820	1096	891	1541	2831	1755
Номера 8 (800)	109	48	55	82	92	69	252	134

* Составлено с использованием источника [5]

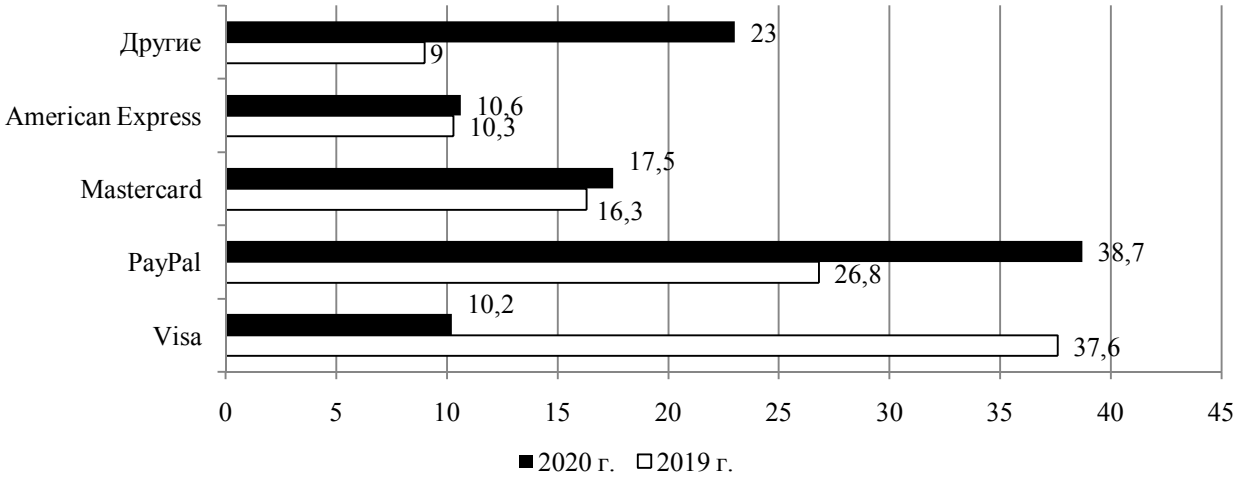

Рис. 5. Бренды платежных систем, используемые в финансовом фишинге, %
** Составлено с использованием источника [6]*

Динамика утечек персональных данных коррелируется с увеличением количества атак с использованием методов социальной инженерии – фишинга. В 2020 г. среди наиболее известных платежных систем мошенниками чаще всего использовался бренд PayPal (38,7 % случаев). Далее отмечаются Mastercard (чья доля незначительно выросла с 16,3 % до 17,5 %), American Express (10,6 %) и Visa (10,2 %) (рис. 5).

В 2020 г. номером один для мошенников был интернет-магазин Amazon (27,84 %), далее – Apple (27,07 %), Steam (14,90%) и eBay (12,85 %) (рис. 6).

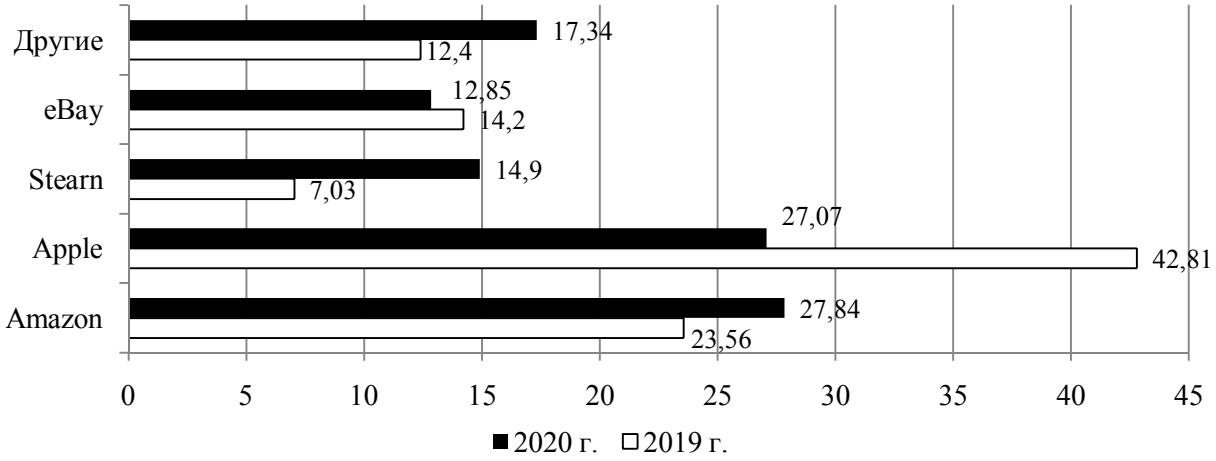

Рис. 6. Бренды интернет-магазинов, используемые в финансовом фишинге, %
** Составлено с использованием источника [6]*

Востребованность дистанционных сервисов и услуг у населения в условиях пандемии выросла, что спровоцировало появление значительного количества ложных сайтов банков. В отчетные периоды ФинЦЕРТ подвергал блокировке преимущественно мошеннические сайты, маскирующиеся под сайты страховых организаций, агентств продажи авиа/железнодорожных билетов, сервисов p2p-переводов, валютно-обменных услуг, а также домены сайтов с ВПО. Всего заблокировано 8469 доменов (рис. 7).

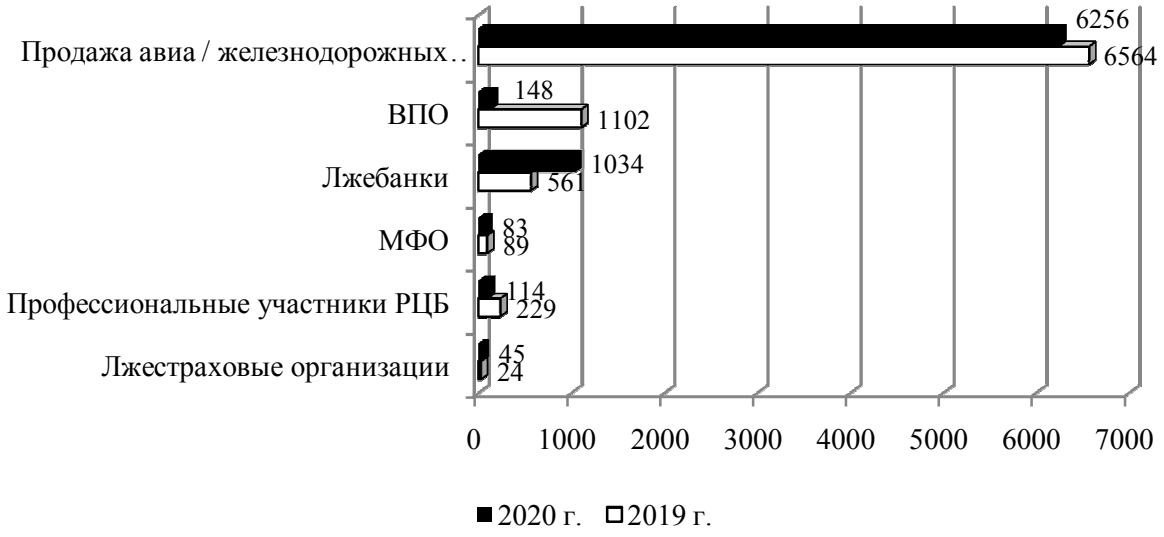

Рис. 7. Блокировка мошеннических ресурсов
** Составлено с использованием источника [5]*

Кредитные организации активно развивают финансовые технологии, позволяющие работать в режиме соблюдения социальной дистанции: блокчейн, искусственный интеллект, интернет вещей и т.д. В то же время цифровая трансформация несет новые риски в области информационной безопасности.

Заключение

Киберпреступность и мошенничество, которые несут угрозу обеспечения экономической безопасности общества, государства и личности являются актуальной проблемой современности. Это обстоятельство стимулирует банки к расширению спектра решений, позволяющих найти компромисс между рисками информационной безопасности и скоростью разработки и вывода новых сервисов на рынок. Отмечается интерес со стороны банков к следующим классам решений: средства контроля привилегированных пользователей, безопасность контейнеризации и Big Data, анализ и безопасность программного обеспечения, внедрение и развитие машинного обучения в части улучшения предоставляемого сервиса и информационной безопасности для отслеживания транзакций. Устойчивой тенденцией является роботизация действий аналитиков при реагировании на инциденты информационной безопасности. Участие кредитных организаций в таких инициативах, как системы быстрых платежей и «цифровой профиль гражданина», а также создание партнерских экосистем требуют от банков новых подходов к обеспечению кибербезопасности. В результате более половины предупреждений об инцидентах безопасности будут обрабатываться автоматически в онлайн-режиме на базе искусственного интеллекта, с использованием поведенческой биометрии и технологии квантового шифрования информации.

Литература

1. Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23.11.2001г.) (в ред. от 28.01.2003г.) [Электронный ресурс]. URL: https://base.garant.ru/4089723/

2. Курманова Д.А., Галимарданов А.Р., Султангареев Д.Р. Цифровая трансформация российского коммерческого банка // Вестник УГНТУ. Наука, образование, экономика. Серия экономика. 2021. № 1. С. 49–61.

3. Курманова Д.А. Стратегия управления безопасностью на рынке инноваций и финансовых технологий // Инновационное развитие экономики. 2019. № 5 (сентябрь-октябрь, часть II). С. 143–147.

4. Николаев В.В., Кулакова Т.А. О тенденциях изменения киберугроз в финансово-кредитной сфере по данным Банка России // Современная наука: Актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 8. С. 102–106.

5. Официальный сайт Центрального банка Российской Федерации [Электронный ресурс]. URL: http: http://www.cbr.ru/

6. Официальный сайт Лаборатории Касперского [Электронный ресурс]. URL: https://www.kaspersky.ru

7. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 11.06.2021 г.).