Елена Александровна ТАРХАНОВА
кандидат экономических наук, доцент, доцент кафедры экономики и финансов Тюменского государственного университета, г. Тюмень, e.a.tarkhanova@utmn.ru
Анжелика Викторовна ФРИЦЛЕР
кандидат экономических наук, доцент, доцент кафедры экономики и финансов Тюменского государственного университета, г. Тюмень, a.v.fricler@utmn.ru

КИБЕРМОШЕННИЧЕСТВО КАК КЛЮЧЕВАЯ УГРОЗА ПРОЦЕССА ЦИФРОВИЗАЦИИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. На протяжении всех этапов исторического развития России банковская сфера представляла собой объект повышенного внимания со стороны злоумышленников, концентрируя в себе огромные финансовые ресурсы. С развитием процесса цифровизации банковской деятельности данный интерес лишь усилился, трансформировавшись под требования цифровой среды. В статье рассмотрено кибермошенничество как ключевая угроза цифровизации банковской деятельности.
Ключевые слова: банковская деятельность, кибермошенничество, коммерческий банк, цифровизация, экономическая безопасность.

Elena Aleksandrovna TARKHANOVA
Candidate of Economic Sciences, Associate Professor of the Department of Economics and Finance at University of Tyumen, Tyumen, e.a.tarkhanova@utmn.ru
Anhelika Viktorovna FRICLER
Candidate of Economic Sciences, Associate Professor of the Department of Economics and Finance at University of Tyumen, Tyumen, a.v.fricler@utmn.ru

CYBER FRAUD AS A KEY THREAT TO THE PROCESS OF BANKING DIGITALIZATION

Abstract. Throughout all stages of the historical development of Russia, the banking sector has been an object of increased attention from malefactors, concentrating huge financial resources. With the development of the process of digitalization of banking activities, this interest has only intensified, transforming to the requirements of the digital environment. The article considers cyber fraud as a key threat to the digitalization of banking.
Keywords: banking, cyber fraud, commercial bank, digitalization, economic security.

На сегодняшний день цифровизация банковской деятельности представляет собой не просто одно из существующий направлений развития коммерческого банка, а основу для удержания его позиций на рынке [1, с. 145]. Несмотря на большое количество преимуществ, которое дает цифровизация кредитным организациям, способствующим вывести их деятельность на новый качественный уровень, важным аспектом выступают вопросы безопасности. [2, с. 146].

Динамика киберпреступлений, возникающих в банковской сфере, бесспорно, сопряжена с цифровизацией экономики и общественных отношений, а также с особенностями киберпространства, связанными и с доступностью информации, и с большим охватом клиентов, а также с анонимностью и трансграничным характером, которые лишь усилились в период пандемии [3].

Исследование киберпреступлений, совершенных в России, свидетельствует о следующих фактах:

– потери россиян от кибермошенников в 2020 г. увеличились на 52% и составили порядка 9,77 млрд руб.;

– более половины рассматриваемых преступлений (58,8% или 300,3 тыс. случаев) совершалось с использованием сети «Интернет», что на 91,3% превышает показатели 2019 г.;

– практически половина (42,9%) преступлений совершалось через средства мобильной связи: 218,7 тысяч инцидентов (+88,3%);

– порядка 5% были совершены с использованием электронных средств платежа, что увеличило их использование в криминальных целях в 6 раз, в частности, совершение преступлений с использованием банковских карт увеличилось на 453,1% (с 34,4 тыс. в 2019 г. до 190,2 тыс. в 2020 г.);

– около 70% совершенных преступлений было связано с мошенничеством;

– порядка 33% преступлений были совершены путем краж с банковских счетов и электронных кошельков, что на 80% превышает показатели 2019 г.;

– одно и то же преступление могло быть совершенно с применением сразу нескольких способов [4].

Анализ количества киберинцидентов в 2020-2021 гг. свидетельствует о сохранении положительной динамики их роста во втором квартале 2021 г. (рис. 1).

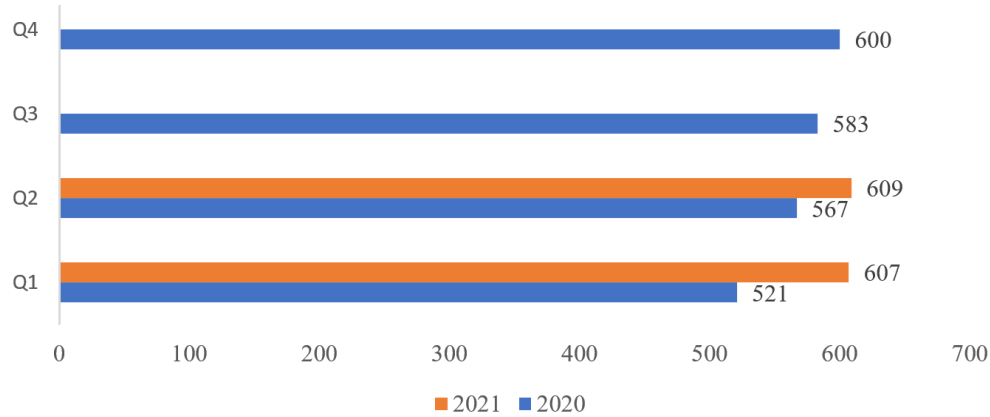

Рис. 1. Количество киберинцидентов в 2020-2021 гг. (по кварталам)

Источник: составлено авторами на основе [5, 6].

Похищенные мошенниками данные позволяют им легко и быстро получить желаемую прибыль путем их продажи через Darknet, что уже стало многофункциональным преступным бизнесом, 80% от оборота которого занимают реквизиты банковских карт, пароли и логины от различных учетных записей [7]. Приобретение размещаемой информации также представляет особую ценность для злоумышленников, поскольку именно она обеспечивает максимальную эффективность применения методов социальной инженерии — главного оружия кибермошенников в отношении населения (рис. 2).

Самым популярным инструментом социальной инженерии по-прежнему остается Vishing, представляющий собой вид атаки, при котором мошенники звонят на телефоны жертв и, притворяясь представителями легитимной орга-

низации (чаще всего банков), узнают конфиденциальную информацию. Особого внимания в данном случае заслуживает подмена номера, которая на сегодняшний день официально признана угрозой национального уровня, поскольку каждый десятый звонок, совершаемый любому гражданину России, по статистике является телефонным мошенничеством [9].

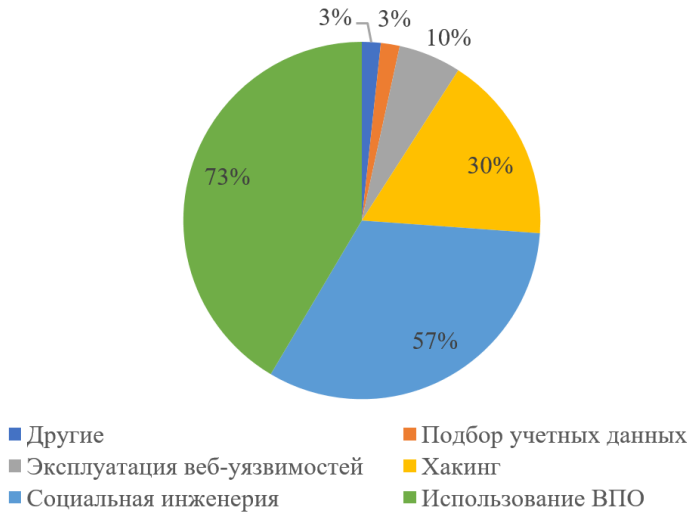

Рис. 2. Структура методов атак злоумышленников в банковской сфере в 2021 г.

Источник: составлено авторами на основе [5, 8].

Важно отметить, что методы социальной инженерии могут быть направлены не только на клиентов банка, но и на их сотрудников. В данном случае ключевым инструментом выступает фишинг, как правило, основывающийся на базе электронной почты и имеющий своей ключевой целью распространение вредоносного программного обеспечения, доля которого составляет порядка 27-30% совершаемых фишинговых рассылок [7].

Помимо этого, представленный вид кибератаки позволяет злоумышленникам получить доступ к переписке представителя банка с клиентами, как правило, содержащей файлы с их персональными данными, а также возможность выйти на диалог с клиентом и запросить необходимую информацию. Ввиду этого основными объектами мошенников становятся сотрудники банков, которые напрямую связаны с обслуживанием клиентов (выдачей кредитов, обслуживанием банковских карт, предоставлением дистанционного доступа, обработкой претензий и др.).

В данном случае безопасность банка напрямую становится зависимой от степени квалификации сотрудников, их осведомленности о возможных проявлениях кибермошенничества, а также от соблюдения ими установленной банком политики безопасности.

Исходя из вышеизложенного, киберугрозы являются на сегодняшний день одной из ключевых угроз процесса цифровизации, поскольку наносят колоссальный ущерб коммерческим банкам: не только финансовый, но и репутационный. Кибермошенничество вырабатывает у людей недоверие к банковской

сфере, что может привести к оттоку клиентов из банков и, как следствие, снижению прибыли и, в крайнем случае, банкротству.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Тарханова Е., Чижевская Е., Бабурина Н. Институциональные изменения и цифровизация бизнес операций в финансовых учреждениях // Журнал институциональных исследований. 2018. Т. 10, № 4. С. 145-155.
2. Тарханова Е.А., Морквина Н.Ю., Стрижова А.А Проникновение цифровых технологий в банковскую сферу Российской Федерации: Ключевые тренды и вызовы // Социально-экономические и гуманитарные науки: сборник избранных статей по материалам Международной научной конференции, Санкт-Петербург, 27 декабря 2020 г. Санкт-Петербург: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2020. С. 146-149.
3. Число киберпреступлений в России // TADVISER: [официальный сайт]. 2005-2021. URL: (дата обращения: 24.02.2022).
4. Состояние преступности в России за январь-декабрь 2020 г. // Министерство внутренних дел Российской Федерации: [официальный сайт]. 2021. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 24.02.2022).
5. Актуальные киберугрозы: II квартал 2021 г. // Positive Technologies: [официальный сайт]. 2002-2021. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/ (дата обращения: 24.02.2022).
6. Всего зарегистрировано преступлений // Портал правовой статистики: [официальный сайт]. URL: http://crimestat.ru/offenses_chart (дата обращения: 24.02.2022).
7. Российская банковская система сегодня: взаимодействие реального и финансового секторов в условиях цифровизации экономики // Ассоциация банков России: [официальный сайт]. 2019. URL: https://asros.ru/upload/iblock/c30/20397_informatsionnoanaliticheskoeobozreniesentyabr2019.pdf (дата обращения: 24.02.2022).
8. Потери банков от киберпреступности // TADVISER: [официальный сайт]. 2005-2021. URL: https://www.tadviser.ru/ (дата обращения: 24.02.2022).
9. Телефонное мошенничество // TADVISER: [официальный сайт]. 2005-2021. URL: https://www.tadviser.ru (дата обращения: 24.02.2022).