УДК 336.77:004.056
DOI 10.35231/25419501_2021_2_59

Зверева М. С.

Угрозы, тренды и субъекты информационной безопасности кредитно-финансовой сферы*

В статье рассмотрены основные и самые опасные атаки групп мошенников в кредитно-финансовой сфере на 2019–2020 гг. Проведен статистический и аналитический анализ изменений ключевых показателей, а также сопоставление их с предыдущим периодом. Результаты исследования могут быть использованы при изучении эффективности использования Банком России инструментов борьбы с киберугрозами. Предполагается, что Центральный Банк Российской Федерации продолжит борьбу с опасными атаками на информацию, разрабатывая для этого новые и эффективные механизмы.

Ключевые слова: Банк России, ВПО, атаки, мошенничество, киберугроза, ФинЦЕРТ.

ГРНТИ: *Экономика / Экономические науки: 06.73.55 Банки.*
ВАК: *08.00.10*

Zvereva M. S.

Threats, trends and subjects of information security in the credit and financial sphere

This article presents the main and most dangerous attacks of fraud groups in the credit and financial industry for 2019–2020. Statistical and analytical analysis of changes in key indicators, as well as their comparison with the previous period, is carried out. The results of the study can be used to explore the effectiveness of the Bank of Russia's use of tools to combat cyberthreats. It is assumed that the Central Bank of the Russian Federation will continue to fight against dangerous attacks on information, developing new and effective mechanisms for this purpose.

Key words: Bank of Russia, HPE, attacks, fraud, cyber threat, FinCERT.

JEL classifications: *G 21*

* Статья подготовлена на основе лучшего секционного доклада X-й всерос. науч.-практ. конф. студентов и аспирантов с международным участием «Проблемы и пути социально-экономического развития: город, регион, страна, мир» (10 июня 2021 г., СПб.: ЛГУ им. А.С. Пушкина). Научный руководитель д-р экон. наук, проф. Космачева Н.М.

Несомненно, новые технологии несут в себе все большие и большие возможности, скорость и комфорт, но в то же время это приносит новые угрозы. В связи с этим актуальными являются мониторинговые и аналитические исследования угроз в разных сферах экономической деятельности, в том числе банковской.

По статистике в 2020 г. мы наблюдаем сокращение попыток компьютерных атак более чем на 40% по сравнению с 2019 г. (рис. 1).

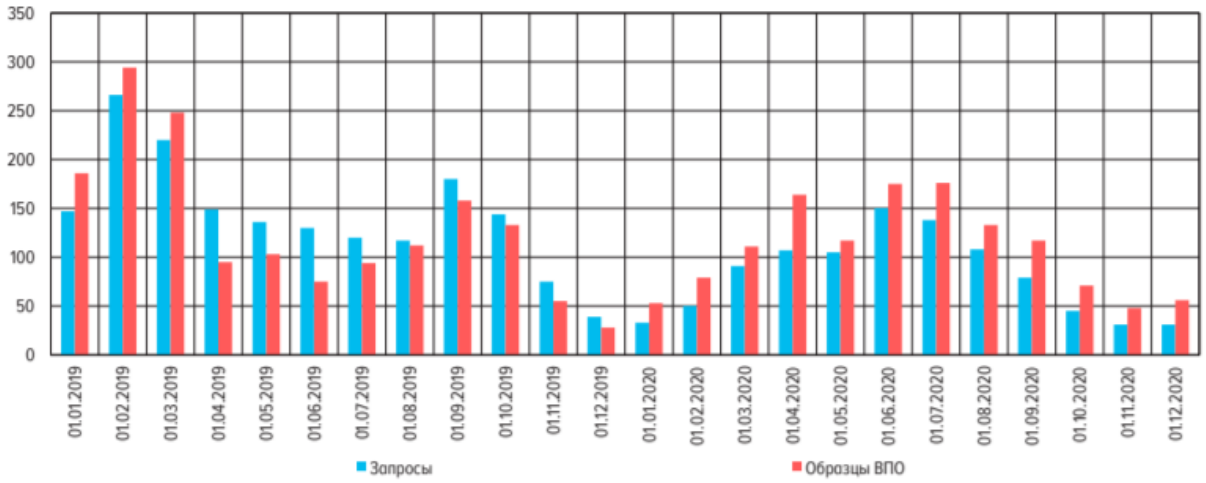

Рис. 1. Поступившие в 2019–2020 гг. запросы о фактах распространения ВПО и исследованные образцы (единиц) [3]

Если рассматривать структуру сфер, в которых происходят вредоносные атаки, то в 2020 г. на первом месте это шпионское ПО, причем увеличение атак составило практически до 45% доли всех операций, а за ним финансовое ПО с долей в 13%. Также, стоит отметить, что в 2020 г. заметно сократились массовые атаки. Связано это с тем, что механизмы Банка России быстрее начали реагировать на пресечение возможных вредоносных программ. Также, ФинЦЕРТ, центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, начал выпускать бюллетени, где прописана вся необходимая информация о самых опасных атаках, способах их обнаружения и противодействия им.

Интересным фактом является и само расположение ресурсов в сети Интернет: все они находятся за пределами Российской Федерации, преимущественно в странах с большим количеством веб-сервисов. Лидерами являются, как и в прошлые годы, США и Германия.

Если же рассматривать атаки на информационную инфраструктуру клиентов организаций кредитно-финансовой сферы РФ, то наиболее активной и опасной угрозой является группа злоумышленников, именуемых как RTM (Remote Transaction Manager). По статистике, за 2019–2020 гг. еженедельно происходило по 2–3 таких атаки, что показывает, насколько интенсивно данные группы людей захватывают информацию пользователей. Большинство случаев относится к фишинговым компаниям, в которых к сообщениям на электронную почту прикрепляется архив с вредоносными ссылками, так называемой «полезной» информацией.

На ряду с уже перечисленными атаками, остаются опасными и атаки на банкоматы. 44% случаев связаны с использованием всевозможных приспособлений для вскрытия дверцы банкомата для извлечения денежных средств. На кеш-треппинг приходится немного меньше: 32% всех случаев.

В связи с последними событиями, а именно с захватившей весь мир коронавирусной инфекцией, начало проявляться все больше случаев кибератак с использованием социальной инженерии. В 84% случаев мошенники использовали для атаки телефонную связь, а в остальных 16% – овладевали личными данными через СМС и сообщения в мессенджерах. На наш взгляд, пандемия оказалась рычагом для активизации мошенников. Так, за 2020 г. показатель количества заблокированных телефонных номеров превышает аналогичный показатель прошлого года на 86%. Анализ показал, что в 57% случаев мошенники представлялись сотрудниками службы безопасности или же сотрудни-

ками той или иной кредитно-финансовой организации. Данное явление является следствием низкой финансовой грамотности населения.

Чаще всего атаки недобросовестных действий происходят с помощью методов социальной инженерии, далее посредством фишинговых рассылок по клиентам банков. По статистике 9 из 10 звонков относятся к теме угрозы накоплениям, либо операциям без согласия клиента.

Таблица 1

Заблокированные по инициативе Банка России мошеннические телефонные номера (ед., по данным Банка России [2])

	2019		2020	
	I квартал	II квартал	I квартал	II квартал
Городские номера	223	1 152	3 473	3 663
Мобильные номера	354	756	891	1 541
Номера 8(800)	109	48	92	69

По состоянию на 2020 г. преобладающим способом мошенничества по телефону остаются звонки по городским номерам. В связи с сложившейся эпидемиологической ситуацией как в стране, так и во всем мире, имеет место расширения рынка предоставления дистанционных услуг. Все больше людей начали искать в сети интернет дистанционные способы привлечения денежных средств, поэтому злоумышленники активизировались и начали создавать различные страницы лжебанков.

Таким образом, объем операций без согласия клиентов составил 4 млрд р., в количестве 361,8 тысяч единиц, при этом доля возмещения составляет лишь 12% в размере 485 млн р.

С развитием технологий и человеческих навыков, все больше людей переходят на оплату в онлайн режиме, в связи с этим мошенников

становится все больше и встает вопрос о защищенности информации при переводе денежных средств.

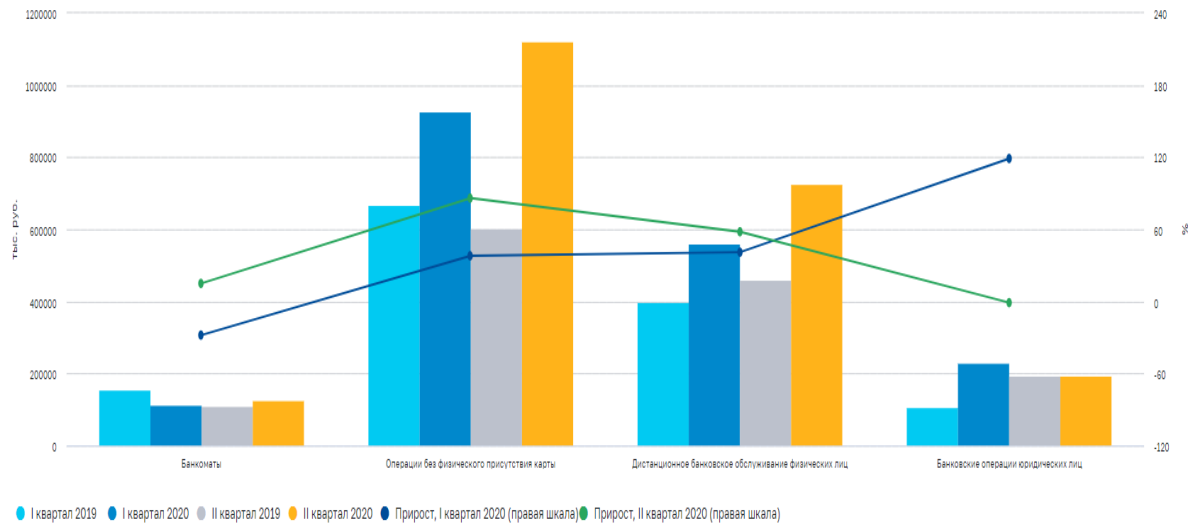

Рис. 2. Объем операций по переводу денежных средств, совершенных без согласия клиентов [2]

По рис. 2 видно, что в I квартале 2020 г. объем операций без согласия клиента вырос по сравнению с тем же показателем 2019 г. на 38%. Возможной причиной такого роста является двукратное снижение общего объема операций с использованием электронного средства платежа. В рамках охватившей весь мир пандемии коронавируса все больше людей начало совершать покупки, используя дистанционные способы оплаты товаров и услуг. Также некоторая часть населения, перешедшего на такую форму оплаты, совершили данные операции впервые. Именно они, в силу своей неопытности, стали наиболее уязвимы при активизировавшихся действиях мошенников.

Во втором квартале 2020 г. наблюдается та же тенденция роста объема операций без согласия клиента, показатель равен +59%. В России в этот период был введен ряд дополнительных ограничений, вследствие чего дистанционные оплаты еще больше увеличились. В этот период наблюдается переход работников на дистанционный ре-

жим работы, что способствовало увеличению доли хищения в системах дистанционного банковского обслуживания юридических лиц.

Банк России активно поднимает тему по обеспечению информационной безопасности, считая, что в период 2021–2023 гг. именно эта сфера будет наиболее развивающейся [4]. К концу планового периода, а именно к 2023 г., им будут введены требования к безопасности управления данными и предотвращение утечек данных из финансовых организаций, произойдет развитие киберкультуры финансового рынка и введение требований к устойчивости деятельности финансовых организаций при реализации киберрисков.

Как основной субъект управления рисками в финансовой среде Банк России должен выполнить важные задачи по подготовке кадров и обеспечению доверия граждан к цифровой среде, осуществлению надзорной деятельности. Этому служат и программы финансовой грамотности, в реализации которых совместно с территориальным управление Центробанка активно участвует ЛГУ имени А.С. Пушкина и его преподаватели [1] и студенты.

Список литературы

1. Космачева Н.М., Бушенева Ю.И. Формирование финансовой грамотности учащихся в контексте компетентностного подхода к обучению // Вестник Ленинградского государственного университета им. А.С. Пушкина. – 2018. – № 4. – С. 321–333.

2. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств / Банк России [Электронный ресурс]. – URL: https://cbr.ru/analytics/ib/review_1q_2q_2020/, свободный (дата обращения: 05.05.2021).

3. Основные типа компьютерных атак в кредитно-финансовой сфере в 2019-2020 годах. Банк России [Электронный ресурс]. – URL: https://cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf, свободный (дата обращения: 05.05.2021).

4. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019-2021 годов / Банк России [Электронный ресурс]. – URL: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf, свободный. (дата обращения: 06.05.2021).

References

1. Kosmacheva N.M., Busheneva Yu.I. *Formirovanie finansovoj gramotnosti uchashchihsya v kontekste kompetentnostnogo podhoda k obucheniyu*. Vestnik Leningradskogo gosudarstvennogo universiteta im. A.S. Pushkina. 2018. № 4. P. 321–333.

2. *Obzor otchetnosti ob incidentah informacionnoj bezopasnosti pri perevode denezhnyh sredstv.* Bank Rossii. URL: https://cbr.ru/analytics/ib/review_1q_2q_2020/.

3. *Osnovnye tipa komp'yuternyh atak v kreditno-finansovoj sfere v 2019-2020 godah*. Bank Rossii. URL: https://cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf.

4. *Osnovnye napravleniya razvitiya informacionnoj bezopasnosti kreditno-finansovoj sfery na period 2019–2021 godov*. Bank Rossii. URL: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf.