УДК 336.71

Т. В. Зайцева, Е. В. Шершова
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты Ростовской области, г. Шахты, email: katrina-2000@list.ru

КИБЕРБЕЗОПАСНОСТЬ КАК НЕОТЪЕМЛЕМЫЙ ИНСТРУМЕНТ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В БАНКОВСКОЙ СФЕРЕ

Ключевые слова: кибербезопасность, киберпреступность, банковская сфера, кибератаки, банк.

В статье рассматриваются особенности кибербезопасности в банковском секторе. Подчеркивается опасность киберпреступлений в данной сфере, что отражает актуальность темы статьи. В работе дается определение кибербезопасности, описываются особенности обеспечения кибербезопасности в банковской сфере, приводятся статистические данные по количеству и объему совершенных кибератак. Также в исследовании выделяются типы киберпреступлений и каналы их совершения. Особое внимание отводится методам, которые способствуют обеспечению должного уровня кибербезопасности, рассматривается процесс проведения комплекса мер по борьбе с киберпреступниками на нормативно-правовом и организационном уровне.

T. V. Zaitseva, E. V. Shershova
Institute of Service Sector and Entrepreneurship (branch) of DSTU in Shakhty, Rostov Region, Shakhty, email: katrina-2000@list.ru

CYBER SECURITY AS AN INTEGRAL TOOL IN COUNTERING CYBER CRIMES IN THE BANKING SPHERE

Keywords: cybersecurity, cybercrime, banking, cyber attacks, bank.

The article examines the features of cybersecurity in the banking sector. The danger of cybercrimes in this area is emphasized, which reflects the relevance of the topic of the article. The paper gives a definition of cybersecurity, describes the features of ensuring cybersecurity in the banking sector, provides statistical data on the number and volume of cyber attacks committed. The study also highlights the types of cybercrimes and the channels for their commission. Particular attention is paid to methods that contribute to ensuring an adequate level of cybersecurity, the process of carrying out a set of measures to combat cybercriminals at the regulatory and organizational level is considered.

В современных условиях наблюдается стремительное развитие цифровых технологий и их активное использование во всех областях человеческой деятельности. Одной из таких сфер является банковская система, в работе которой ежедневно применяются современные компьютерные технологии. В рамках цифровизации многие банки создают новые виды продуктов и услуг, улучшают уже существующие технологии. Кроме того, в связи с пандемией COVID-19 увеличилась доля безналичных расчетов и дистанционного банковского обслуживания. Поэтому функционирование банков находится в большой зависимости от правильной и бесперебойной работы информационных и компьютерных технологий.

Однако применение цифровых технологий вместе со значительными преимуществами влечет за собой и определенные опасности, одной из которых является киберпреступность. Банковский сектор из-за имеющихся активов, оборота огромной суммы денежных средств, осуществления большого количества транзакций и наличия клиентских данных считается главной мишенью преступников. По этой причине все большую актуальность приобретает кибербезопасность, которая направлена на предупреждение и предотвращение мошеннических операций.

Цель исследования

Цель данного исследования заключается в изучении видов банковских киберпреступлений, рассмотрении инструментов и методов, используемых как кредитно-финансовыми учреждениями, так и их клиентами для обеспечения

кибербезопасности в банковской сфере и нейтрализации последствий от различных видов кибератак.

Материал и методы исследования

При проведении исследования использовались общенаучные методы исследования, а именно статистический, сравнительный и логический анализ. Кроме перечисленных методов в статье также применялся графический метод визуализации данных для того, чтобы наглядно представить результаты исследования. Материалом для данной работы послужили нормативно-правовые акты, обзоры отчетности об инцидентах информационной безопасности при переводе денежных средств в период с 2019 года по 2 квартал 2021 года.

Результаты исследования и их обсуждение

Кибербезопасность представляет собой совокупность методов по защите программ, сетей и систем от кибератак злоумышленников, нацеленных на получение доступа к конфиденциальной информации. Осуществления эффективных мер для защиты активов и виртуальных данных выступает ключевым условием для реализации успешной работы банковского сектора.

По данным таких российских банков, как Сбербанк и ВТБ, в 2021 году отмечается увеличение кибератак на информационную инфраструктуру банков. Так, ВТБ зафиксировал за пять месяцев 2021 года 1,2 млн попыток кибератак. В Сбербанке сообщают о том, что с января по апрель 2021 года количества DDoS-атак (атака, направленная на отказ оборудования в обслуживании) увеличилось в 4 раза по сравнению с 2020 годом [1].

В 2020 году Центральным Банком было зафиксировано 130 успешных атак мошенников на системы банков с общей суммой ущерба в 35 млн рублей. Эти значения превышают показатели 2019 года: число успешных кибератак – 58, а общая сумма ущерба – 26,2 млн рублей.

Однако, несмотря на рост кибератак, банки хорошо справляются с киберпреступностью и защищены от прямого вывода денежных средств, в отличие от своих клиентов. Согласно информации Центрально Банка, объем украденных денежных средств у банковских клиентов в 2020 году составил 9 млрд. рублей [2]. Так, Банк «Открытие» отметил, что наблюдается рост кибератак именно на клиентов, а не на банковские системы.

По данным Центрального Банка, за 2 квартал 2021 года произошло 236,971 тыс. несанкционированных операций по банковским счетам клиентов на сумму 3,013 млрд рублей, это на 44,335 тыс. операций и соответственно 836 млн рублей больше, чем за 2 квартал 2020 года (табл. 1). Таким образом, число операций без согласия клиентов во 2 квартале 2021 года увеличилось на 23% относительно аналогичного периода 2020 года, а рост количества несанкционированных операций по банковским счетам клиентов во 2 квартале 2020 году по сравнению с тем же периодом 2019 года составил 70%.

Данные, приведенные в таблице 1, наглядно показывают, что с каждым годом количество и объем несанкционированных операций по банковским счетам клиентов увеличиваются. Данный рост объясняется тем, что население в период пандемии стало активно использовать дистанционные способы потребления продуктов и услуг, в том числе финансовых, а организации начали переходить на удаленный формат работы. То есть увеличение общего объема операций с использованием электронного средства платежа поспособствовало росту объема несанкционированных операций по банковским счетам.

Наибольшее число мошеннических операций в разрезе каналов совершения операций были осуществлены через системы оплаты товаров и услуг в Интернете: в 2021 году – 166 734 несанкционированные операции, в 2020 году – 153 101 (рис. 1). На втором месте по количеству операций, совершенных без согласия клиента, находятся операции, которые были проведены в системе дистанционного банковского обслуживания физических лиц: в 2021 году – 48 882 несанкционированные операции, в 2020 году – 29 270. Также стоит отметить, что число мошеннических операций через все виды каналов увеличилось за рассматриваемый период времени.

Таблица 1

Число и объем операций без согласия клиентов по годам [3]

Показатель	2021		2020		2019	
	2 кв.	1 кв.	2 кв.	1 кв.	2 кв.	1 кв.
Число операций без согласия клиентов, ед.	236 971	237 737	192 636	169 501	113 250	124 788
Объем операций без согласия клиентов, млн руб.	3 013	2 873	2 177	1 830	1 368	1 328

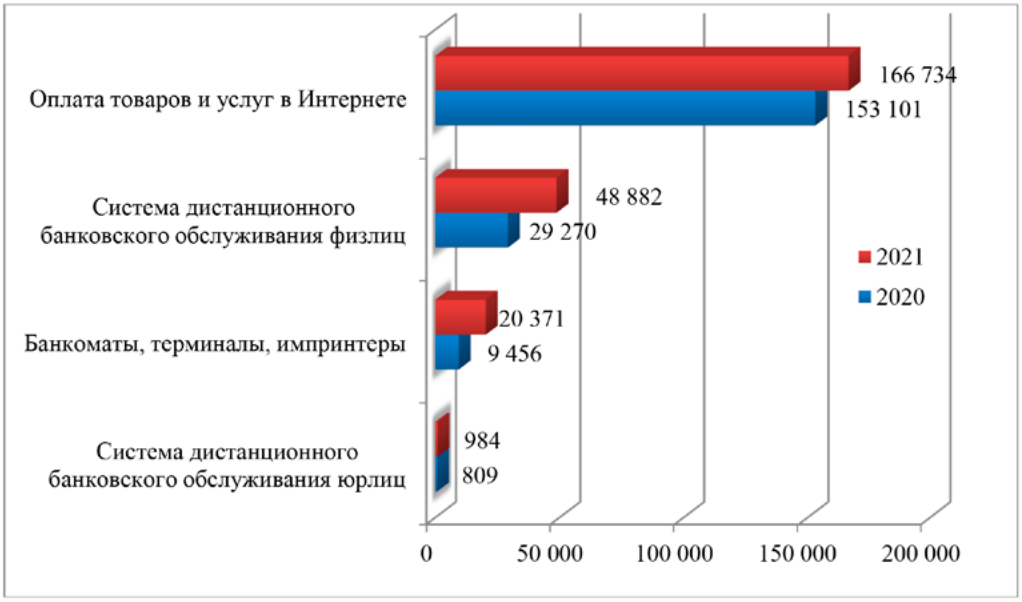

Рис. 1. Количество операций без согласия клиентов во 2 квартале, распределенные по каналам совершения операций, ед. [3]

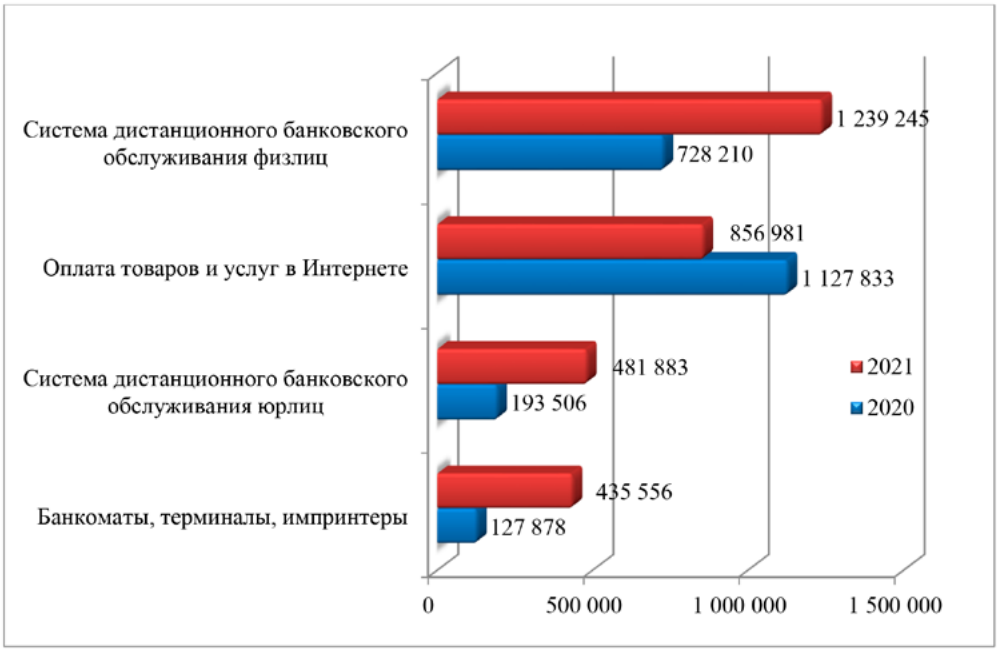

Рис. 2. Объем операций без согласия клиентов во 2 квартале, распределенные по каналам совершения операций, тыс. рублей [3]

Лидером по объему хищений в разрезе каналов совершения операций в 2021 году является система дистанционного банковского обслуживания физических лиц – 1 239,245 млн рублей (рис. 2). Рост данного канала совершения несанкционированных операций в 2021 году относительно 2020 года составил 70%. На втором месте по объему операций без согласия клиентов находится операции по оплате товаров и услуг в Интернете – 856,981 млн рублей. Однако объем хищений, полученных с помощью данного канала совершения несанкционированных операций за рассматриваемый период, снизился относительно прошлого года на 270,852 млн рублей.

Для поддержания безопасности информационных данных необходимо противодействовать киберпреступности. В первую очередь для обеспечения кибербезопасности необходимо знать, какие бывают финансовые кибератаки, и уметь их выявлять. К киберпреступлениям в банковской сфере относятся:

− Социальная инженерия – способ психологического манипулирования людьми с целью получения преступником от клиентов финансовой организации конфиденциальной информации, необходимой для хищения денежных средств с банковских карт. Иными словами, клиент банка, будучи введен в заблуждение аферистом, самостоятельно сообщает свои персональные данные злоумышленнику, представившемуся, например, сотрудником банка, социальной службы или полиции.

− Фишинг чаще всего представляет собой ситуацию, когда сам пользователь на сайте, созданном мошенниками, вводит данные своей банковской карты (включая код безопасности CVV, пин-код). Такие сайты, созданные злоумышленниками, очень похожи на официальные сайты банков или магазинов, а разница обычно находится в адресе. Например, вместо alfabank.ru может быть alfabamk.ru, а вместо paypal.com – paypai.com. После введения своих персональных данных на таких сайтах у держателей банковских карт похищаются номера карты, CVV/CVC– и ПИН-коды.

− Эксплуатация уязвимостей программного обеспечения заключается в том, что мошенники используют уязвимости банковских приложений с целью похищения денежных средства их пользователей. Большинство банковских сервисов имеют высокий уровень защищенности, однако в некоторых банковских системах безопасности встречаются бреши и недочеты, которыми могут воспользоваться киберпреступники. К недостаткам мобильного банкинга относится незащищенность операционной системы – в некоторых версиях Android есть вероятность перехвата соединения мобильного приложения с банком при помощи вируса. Это позволяет мошенникам получить контроль над зараженным приложением и производить операции без согласия владельца счета [4].

− DDoS атака – способ нарушить работоспособность инфраструктуры компании и клиентских сервисов путем подачи большого количества запросов. Для проведения данных атак чаще всего используют ботнет, представляющий собой сеть компьютеров, на которых скрытно установлено вредоносное ПО, позволяющее хакерам управлять вычислительными ресурсами зараженных устройств удаленно.

Согласно данным Центрального Банка, наибольшее число кибератак на клиентов банков совершено с использованием методов социальной инженерии. Во 2 квартале 2021 года их количество составило 11 173 атаки, что на 143,47% больше, чем годом ранее (табл. 2). На втором месте находятся фишинговые атаки: во 2 квартале 2021 года их насчитывалось 1 160, а в 2 квартале 2020 года – 583. Количество атак с использованием вредоносного программного обеспечения (атаки, направленные на финансовые организации) практически не изменилось за год. Число атак с использованием эксплуатации уязвимостей программного обеспечения уменьшилось на 69,89% во 2 квартале 2021 года относительно 2 квартала 2020 года.

Значительную роль в противодействии киберпреступлениям играет понимание того, как можно выявить и предотвратить данный вид мошенничества. К основным способам обеспечения кибербезопасность в банковской сфере можно отнести постоянный мониторинг и своевременное обновление защитных систем.

Таблица 2

Количество кибератак по типам [3]

Инциденты по типам атак	2021, 2 квартал	2020, 2 квартал	Абсолютное изменение, ед.	Темп прироста, %
Атаки с использованием методов социальной инженерии	11173	4589	6584	143,47
Фишинговые атаки	1160	583	577	98,97
Атаки с использованием вредоносного программного обеспечения (атаки, направленные на финансовые организации)	112	103	9	8,74
Эксплуатация уязвимостей программного обеспечения	56	186	-130	-69,89
Остальные инциденты	251	113	138	122,12

Кроме того, большое значение в осуществлении кибербезопасности имеет и обратная связь кредитно-финансовых учреждений с организациями, которые занимаются поиском и устранении киберугроз, а также с государственными органами, выявляющими и привлекающими мошенников к ответственности.

Роль финансового регулятора в России исполняет Центральный Банк, который посредство своих структурных подразделений обеспечивает кибербезопасность кредитно-финансовых учреждений, осуществляет мониторинг их киберустойчивости, предоставляет информацию о новых видах угроз, устанавливает необходимый набор требований по защите от киберугроз.

Важным звеном системы обеспечения кибербезопасности банковской сферы является законодательное регулирование. Основные меры по защите информации установлены национальным стандартом ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций [5]. Защита информации финансовых организаций. Методика оценки соответствия». Качество реализации данных мер с января 2021 года оценивается внешним аудитором в соответствии с Положением Банка России от 09.06.2012 № 382-П, а также Положением Банка России от 17.04.2019 № 683-П [6,7].

Банковскому сектору для обеспечения должного уровня кибербезопасности следует проводить борьбу с киберпреступниками не только на нормативно-правовом, но и на организационном уровне. Так, для успешного предотвращения кибератак банкам следует применять аппаратные, программные и программно-аппаратные комплексы средств защиты информации; усиливать защищенность банковских сервисов и не допускать уязвимости в мобильных банковских приложениях; обучать работников банков основам информационной безопасности и обеспечивать защиту рабочих мест сотрудников от кибератак. Также важно осуществлять сотрудничество специалистов сферы кибербезопасности с представителями банковского сектора.

Для обеспечения кибербезопасности особое внимание стоит уделить повышению цифровой грамотности клиентов банка, оповещению их о различных видах киберугроз. Клиенты банка чаще всего становятся жертвами киберпреступников, именно поэтому население должно знать о видах киберпреступлений, понимать, как правильно поступать в случае киберугрозы, а банки, в свою очередь, должны постоянно проводить мониторинг и при обнаружении пресекать данные правонарушения.

Таким образом, обеспечение кибербезопасности в современных условиях является одним из основных условий поддержания экономической безопасности и конкурентоспособности в стране. Применение комплекса мер по борьбе с киберпреступлениями и своевременная оценка уровня кибербезопасности положительным образом отразятся на банковском секторе, и, следовательно, на всей экономике в целом.

Библиографический список

1. Банки фиксируют рост кибератак на свои системы. [Электронный ресурс]. URL: https://www.vedomosti.ru/finance/articles/2021/07/05/877001-banki-fiksiruyut-kiberatak (дата обращения: 11.10.2021).

2. ЦБ: Потери клиентов банков от кибермошенников выросли в полтора раза. [Электронный ресурс]. URL: https://rg.ru/2021/03/11/cb-poteri-klientov-bankov-ot-kibermoshennikov-vyrosli-v-poltora-raza.html (дата обращения: 10.10.2021).

3. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/review_2q_2021/ (дата обращения: 10.10.2021).

4. Безопасность зависит и от пользователя»: стоит ли доверять банковским приложениям. [Электронный ресурс]. URL: https://www.gazeta.ru/tech/2021/03/11/13507922/mobile_banking.shtml (дата обращения: 11.10.2021).

5. ГОСТ Р 57580.2-2018. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия (утв. и введен в действие Приказом Росстандарта от 28.03.2018 N 156-ст). [Электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=19415#b8aDPmScFoKwWwmf2 (дата обращения: 12.10.2021).

6. Положение Банка России от 09.06.2012 N 382-П (ред. от 07.05.2018) «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_131473/ (дата обращения: 12.10.2021).

7. Положение Банка России от 17.04.2019 N 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_324968/ (дата обращения: 12.10.2021).