УДК 004+336.717

ДИСТАНЦИОННЫЕ ЦИФРОВЫЕ СЕРВИСЫ В БАНКОВСКОМ СЕКТОРЕ РОССИИ: РИСКИ РАЗВИТИЯ И ПУТИ ИХ ПРЕОДОЛЕНИЯ

Зинина О.С.

к.э.н., доцент

Кубанский государственный аграрный университет имени И.Т. Трубилина

г. Краснодар, Россия

Денисова О.Г.

студентка

Кубанский государственный аграрный университет имени И.Т. Трубилина

г. Краснодар, Россия

Аннотация

Исследование посвящено анализу и оценке развития дистанционных цифровых сервисов в банковском секторе России. Авторами выявлены ключевые тенденции развития цифровых сервисов в банковской сфере России в условиях диджитализации экономики страны. Определены и охарактеризованы риски, связанные с цифровизацией банковской деятельности в России. На основе результатов проведенного анализа разработаны и определены наиболее эффективные мероприятия, которые позволят минимизировать число мошеннических операций в условиях цифрового банкинга.

Ключевые слова: дистанционный банкинг, цифровые сервисы, цифровизация, искусственный интеллект, социальная инженерия, фишинг, финансовая грамотность.

REMOTE DIGITAL SERVICES IN THE RUSSIAN BANKING SECTOR: DEVELOPMENT RISKS AND WAYS TO OVERCOME THEM

Zinisha O.S.
candidate of Economics, associate professor
Kuban State Agrarian University named after I.T. Trubilin
Krasnodar, Russia

Denisova O.G.
student
Kuban State Agrarian University named after I.T. Trubilin
Krasnodar, Russia

Abstract
The research is devoted to the analysis and evaluation of the development of remote digital services in the banking sector of Russia. The authors have identified key trends in the development of digital services in the banking sector of Russia in the conditions of digitalization of the country's economy. The risks associated with the digitalization of banking activity in Russia are identified and characterized. Based on the results of the analysis, the most effective measures have been developed and identified that will minimize the number of fraudulent transactions in digital banking.

Keywords: remote banking, digital services, digitalization, artificial intelligence, social engineering, fishing, financial literacy.

Современный мир невозможно представить без цифровых продуктов, которые вошли практически во все сферы деятельности. Банковский сектор является наиболее ярким примером применения дистанционных цифровых сервисов. Его диджитализация осуществлялась размерено, однако в период

пандемии коронавируса возникла необходимость в ускорении этих процессов. В 2020 году кредитные организации активно занялись разработкой новых и совершенствованием традиционных цифровых продуктов, и вскоре представили их своим клиентам.

Многие дистанционные сервисы, предложенные российскими банками, оказались привлекательными не только их клиентам, но и мошенникам, которые стремятся завладеть персональными данными. В коронавирусный период, когда многие сотрудники были переведены на самоизоляцию и оказались вынуждены осуществлять банковские операции с использованием электронных средств, активизировалась и работа злоумышленников, пытающихся получить доступ к их денежным средствам. Необходимость разработки мероприятий, которые позволят предупреждать риски несанкционированного доступа к персональным данным клиентов российских банков, обусловливает актуальность темы исследования.

Условия 2020 года, в которых оказались все российские организации, ускорили процессы внедрения дистанционных цифровых услуг. Так, одной из тенденций развития современного цифрового банковского мира стало применение искусственного интеллекта (ИИ) для снижения нагрузки сотрудников кредитных организаций. Особенность использования технологии искусственного интеллекта в банковской деятельности заключается в упрощении работы с клиентами благодаря компьютерным алгоритмам, которым обучается искусственный интеллект для решения различных задач [1]. Кроме того, в целях обеспечения информационной безопасности широко стала применяться биометрия, которая в банковской среде представляет собой инструмент, предоставляющий клиенту доступ к денежным средствам при подтверждении его личности по отпечатку, голосу, лицу и др. [2].

Еще одной тенденцией развития цифровой банковской системы стал рост числа бесконтактных операций или online-операций, поскольку период

самоизоляции перенес все операции, связанные с движением денежных средств, в online-пространство [3]. Однако все это привело к росту числа мошеннических операций.

Во время карантинных условий, когда большая часть населения работала дистанционно, мошенники решили вернуться к способу хищения денежных средств клиентов банков посредством телефонных звонков. Согласно данным ФинЦЕРТа, 84 % случаев атак с использованием социальной инженерии в 2019-2020 гг. были осуществлены посредством звонков [5].

Ключевыми каналами воздействия на жертв в 2020 году стали online-платформы для покупки и продажи товаров «Авито» и «Юла». В 83 % атак мошенники пользовались данными сервисами для хищения денежных средств пользователей. Лишь 15 % атак совершались через SMS-сообщения, что карта заблокирована, поскольку этот сценарий преимущественно реализовывался посредством телефонных звонков потенциальной жертве с предлогом перевести денежные средства на «безопасный счет» [5].

Еще одним инструментом социальной инженерии, который активно применялся в период самоизоляции, выступил фишинг, который состоит в том, что мошенник создает точную копию сайта кредитной организации или иной структуры для получения доступа к персональным данным жертвы [6]. Наиболее активная фаза применения фишинга в России наблюдалась летом 2020 года, когда Президент страны В.В. Путин объявил о предоставлении единовременных выплат семьям с детьми. На рисунке 1 представим корреляцию числа новостей о социальных выплатах и фишинговых сайтов.

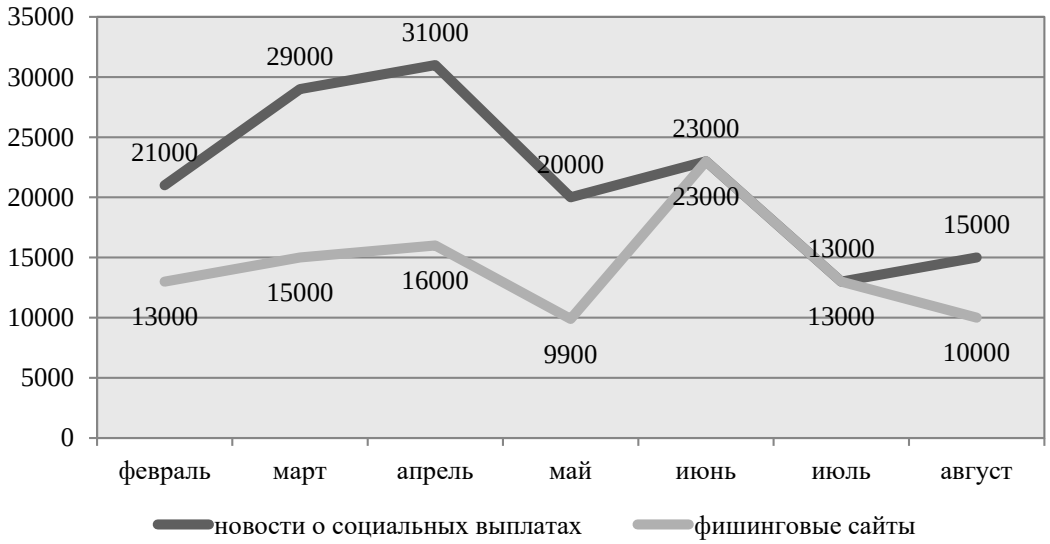

Рис. 1 – Корреляция числа новостей о социальных выплатах и фишинговых сайтов в 2020 году, согласно ФинЦЕРТу, ед. [5]

На рисунке 1 наглядно прослеживается рост числа фишинговых сайтов после объявления выплат в размере 10 тыс. руб. в июне 2020 года. Мошенники воспользовались ситуацией, когда население еще не располагало необходимой информацией о порядке получения выплат, и создали фишинговые сайты для привлечения потенциальных жертв.

Компьютерные атаки, которые зародились в эпоху развития глобальной сети Internet, также стали неотъемлемой частью развития цифрового банкинга. Сущность компьютерных атак в основном заключается в установке вредоносного программного обеспечения (ВПО) на устройство жертвы и получения благодаря нему всей необходимой информации [4].

Исследование показало, что по признаку числа пользователей-получателей ВПО к 2020 г. атаки с применением вредоносных программ стали в большей степени немассовыми. Специалисты ФинЦЕРТа считают, что меры безопасности и реагирования на мошеннические операции совершенствуются, по этой причине число массовых атак становится меньше [5].

Департамент информационной безопасности ФинЦЕРТа призван минимизировать риски и предотвратить угрозу хищения персональных данных клиентов. В связи с этим Банк России разрабатывает нормативно-правовые условия совершенствования коммерческими банками и иными кредитными организациями антифрод-систем. Ниже представим предлагаемые мероприятия по управлению рисками, которые сопровождают дистанционное банковское обслуживание.

Одной из мер предупреждения рисков, связанных с использованием дистанционных цифровых сервисов, в частности телефонного мошенничества, может стать внедрение функции видеозвонка в официальном мобильном приложении банка как средства общения сотрудника и клиента. Предлагаемая инновация позволит клиентам идентифицировать работника кредитной организации, поскольку звонок совершается посредством мобильного приложения банка.

Борьба с фишинговыми сайтами продолжается уже много лет, однако разработать эффективные методы их устранения достаточно трудно. В рамках данного исследования Банку России предлагается создать мобильное приложение с применением обученного искусственного интеллекта, к которому граждане смогут обращаться при обнаружении подозрительного сайта. Искусственный интеллект после проверки будет осуществлять блокировку подобных сайтов.

В рамках противодействия фишингу как наиболее популярной схеме мошенничества также необходимо совершенствовать нормативно-правовую базу его регулирования. Предлагается внести понятие «фишинг» в Уголовный кодекс Российской Федерации и определить меру наказания.

Развитие дистанционных цифровых сервисов в банковской сфере привело к формированию множества угроз различного характера, которые обычным пользователям могут быть неизвестны. Рекомендуется в мобильных

приложениях кредитных организаций включить бесплатные push-уведомления со статьями о новых методах мошенничества и возможных направлениях предотвращения подозрительных операций.

Немаловажным направлением предотвращения риска совершения мошеннической операции, связанной с использованием цифровых банковских сервисов, остается также совершенствование мероприятий по повышению уровня финансовой грамотности населения страны. Следует размещать сведения о новых мошеннических схемах во всевозможных источниках.

Таким образом, проведенное исследование позволило определить, что мошеннические схемы, направленные на получение доступа к личным данным банковских клиентов, ежегодно совершенствуются и, несмотря на значительное развитие методов обеспечения информационной безопасности в банковской сфере, клиенты всегда должны полагаться на себя. Внимательность является главным фактором, который позволит избежать хищения денежных средств клиента злоумышленниками.

Библиографический список:

1. Бутенко, Е. Д. Искусственный интеллект в банках сегодня: опыт и перспективы / Е. Д. Бутенко // Дайджест-финансы. – 2020. – Т. 25. – № 2 (254). – С. 230-242.

2. Ганижева, Н. Ж. Обеспечение информационной безопасности банковской системы / Н. Ж. Ганижева // Студенческий. – 2022. – № 1-1 (171). – С. 61-62.

3. Грязнов, С. А. Перспективы развития дистанционного банковского обслуживания / С. А. Грязнов // Тенденции развития науки и образования. – 2021. – № 69-3. – С. 39-42.

4. Могунова, М. М. Понятие современной киберпреступности и способы совершения финансово-ориентированных киберпреступлений / М. М. Могунова

// Вестник Омского университета. Серия: Право. – 2022. – Т. 19. – № 1. – С. 80-86.

5. Основные типы компьютерных атак в кредитно-финансовой сфере в 2019-2020 годах [Электронный ресурс]. – Режим доступа: URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf. (дата обращения: 16.02.2022).

6. Mammadov, M. İ. Research of methods for determining information attacks on Computer networks / M. İ. Mammadov, U. E. Safarova // Актуальные научные исследования в современном мире. – 2021. – No 11-1 (79). – P. 13-17.

Оригинальность 90%