Научная статья
УДК 343.9
EDN TIELEE
DOI 10.17150/2500-4255.2023.17(4).383-391

ПРЕДУПРЕЖДЕНИЕ МОШЕННИЧЕСТВ В БАНКОВСКОЙ СФЕРЕ

Л.А. Петрякова[1, 2]
[1] Иркутский государственный университет, г. Иркутск, Российская Федерация
[2] Байкальский государственный университет, г. Иркутск, Российская Федерация

Информация о статье

Дата поступления
5 июня 2023 г.

Дата принятия в печать
24 августа 2023 г.

Дата онлайн-размещения
18 сентября 2023 г.

Ключевые слова

Предупреждение мошенничеств; мошенничества в банковской сфере; личность мошенника; специально-криминологические меры предупреждения; антифрод-система

Финансирование

Исследование проведено при финансовой поддержке гранта Иркутского государственного университета № 091-23-333 «Особенности детерминации и предупреждения мошенничеств в банковской сфере»

Аннотация. В статье на основе проведенного исследования сформулированы предложения по предупреждению мошенничеств в банковской сфере. Целью настоящего исследования является разработка практических рекомендаций по совершенствованию уже существующей системы предупреждения мошенничеств в банковской сфере и повышение ее эффективности. В рамках организационно-управленческих мер предлагается повысить уровень межведомственного взаимодействия правоохранительных органов с банками и иными кредитными организациями; осуществлять тщательный подбор, обучение и адаптацию кадров органов финансово-кредитного контроля, так как польза от хорошо обученного сотрудника в офисе банка неоценима. Особое внимание обращается на необходимость борьбы с «утечками» персональных данных клиентов банка. Технические меры позволяют решать большую часть проблем в борьбе с банковским мошенничеством, поэтому следует разрабатывать и совершенствовать системы, которые способны адаптироваться к новым схемам мошенничества. В рамках уголовно-правовых мер предлагается исключить из уголовного закона специальные составы ст. 159.1 и 159.3 УК РФ, перенеся ответственность за данные преступления в общий состав мошенничества. Для повышения уровня защищенности жертв банковского мошенничества следует проводить профилактическую работу с лицами, обладающими возрастной и ролевой виктимностью; повышать уровень цифровой, финансовой и технической грамотности потенциальных и реальных потерпевших в целях профилактики рецидива их виктимности; информировать о новых способах совершения мошенничеств. Обращается внимание на то, что жертвой банковского мошенника может выступать как физическое, так и юридическое лицо, поэтому следует учитывать специфику потерпевшего при построении мер профилактики. Указывается, что активная работа в обозначенных направлениях является, на наш взгляд, важным шагом на пути эффективного выявления и предупреждения мошенничеств в банковской сфере.

Original article

PREVENTION OF FRAUD IN THE BANKING SECTOR

Lyudmila A. Petryakova[1, 2]
[1] Irkutsk State University, Irkutsk, the Russian Federation
[2] Baikal State University, Irkutsk, the Russian Federation

Article info

Received
2023 June 5

Accepted
2023 August 24

Available online
2023 September 18

Keywords

Fraud prevention; fraud in the banking sector; identity of the fraudster; special measures of criminological prevention; anti-fraud system

Abstract. The author uses the conducted research to formulate suggestions on preventing fraud in the banking sector. The goal of the study is to develop practical recommendations on improving the existing system of preventing fraud and enhancing its effectiveness. Within organizational and managerial measures, it is recommended to improve the inter-agency cooperation between law enforcement bodies and banks and other credit organizations; to carry out a thorough selection, training and adaptation of employees for the financial-credit supervision bodies, as the usefulness of a well-trained bank employee is difficult to overestimate. Special attention is paid to the necessity of counteracting "leaks" of bank clients' personal data. As technical measures make it possible to solve most problems of counteracting bank fraud, the systems capable of adaptation to the new fraud schemes should be designed and improved. Within criminal law measures, it is suggested that special crimes of Art. 159.1 and 159.3 of the Criminal Code of the Russian Federation

ISSN 2500-1442

Acknowledgements
The study was financially supported by the Irkutsk State University Grant No. 091-23-333 «Peculiarities of Identification and Prevention of Fraud in the Banking Sector»

should be excluded from criminal law, and liability for them should be transferred to the general crime of fraud. To improve the protection level for victims of bank fraud, it is recommended to conduct preventive work with persons characterized by age and role victimity; to raise the level of digital, financial and technical literacy of potential and actual victims in order to prevent repeat victimity; to provide information about new ways of committing crimes. It is stressed that both physical and juridical persons could be victims of bank fraud, so the specific features of the victim should be considered in the development of prevention measures. It is pointed out that active work in these directions is, according to the author, an important step towards effective identification and prevention of fraud in the banking sector.

Вопросом противодействия мошенничествам в кредитно-банковской сфере в отечественной науке занимались разные ученые до разделения мошенничеств на виды в 2012 г. [1–3]. Однако с тех пор в значительной степени изменилась как сама общественная ситуация (пандемия и связанные с ней ограничения, цифровизация жизни общества, введение санкций, из-за проведения Россией СВО на территории Украины), так и факторы ее детерминирующие. Методы же противодействия преступлениям должны соответствовать современному состоянию криминогенной ситуации. В этой связи необходим новый подход к профилактике и борьбе с мошенничествами в данной сфере.

Исходя из анализа факторов совершения мошенничеств в банковской сфере, предлагаем следующие специально-криминологические меры противодействия.

Прежде всего, необходимо повысить уровень межведомственного взаимодействия правоохранительных органов с банками и иными кредитными организациями, поскольку грамотно организованное взаимодействие с контрольными и надзорными органами во многом повышает эффективность борьбы с преступлениями.

По мнению некоторых авторов, эта проблема, заслуживает отдельное самостоятельное научное исследование [4, с. 73; 5, с. 135].

Президент Российской Федерации в 2022 г. подписал закон[1] об информационном взаимодействии Центрального Банка России и МВД России, который создает условия для автоматизированного обмена данными между ведомствами. Закон будет способствовать повышению скорости расследования дел по фактам мошенничества при денежных переводах.

Ранее при рассмотрении таких дел затрачивалось значительное время на запросы данных и переписку между правоохранительными органами и банками. Согласно принятому закону МВД будет подключено к автоматизированной системе ФинЦЕРТ Банка России, в которой содержится информация об операциях, проведенных без согласия клиентов, что позволит правоохранителям практически в онлайн-режиме получать сведения о мошеннических операциях. Обмен данными будет осуществляться с соблюдением всех норм банковской тайны. В свою очередь МВД России будет передавать в базу ФинЦЕРТ сведения о совершенных преступлениях, которые банки смогут учитывать в своих бизнес-процессах для предотвращения мошеннических переводов. Закон вступит в силу только 21 октября 2023 г., а до этого момента будет подписано двустороннее соглашение, которое определит виды сведений, порядок, сроки и формат их передачи, а также позволит интегрировать информационные системы.

Безусловно, закон заслуживает внимания и поддержки, поскольку направлен на защиту интересов потерпевших от преступлений, связанных с переводами денежных средств без согласия клиента. Тем не менее в нем имеется существенная неопределенность относительно защиты охраняемой законом тайны. Передача Банком России соответствующей информации будет осуществляться на основании сведений МВД России о совершенных противоправных деяниях. При этом порядок обмена информацией, форма и перечень предоставляемых сведений будут определяться межведомственным соглашением между Банком России и МВД России, именно оно определит форму и порядок взаимодействия (предполагается оперативный информационный обмен посредством автоматизированной системы).

Полагаем, что отсутствие в законопроекте исчерпывающего перечня оснований для на-

[1] О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 27 Федерального закона «О национальной платежной системе» : федер. закон от 20 окт. 2022 г. № 408-ФЗ // Российская газета. 2022. № 240.

правления запроса, сведений о должностных лицах, уполномоченных на его формирование и получение соответствующей информации, оставляет вопросы об уровне обеспечения защиты персональных данных, банковской тайны и иной тайны при обмене информации между ведомствами. Поэтому представляется, что для разрешения подобных ситуаций необходимо установить закрытый перечень лиц из числа сотрудников правоохранительных органов, которые будут иметь право доступа к сведениям, составляющим банковскую тайну (в том числе на электронных носителях), а также установить конкретные сроки предоставления информации, предусмотрев возможность их увеличения по просьбе банков.

Следующей группой мер является проведение мероприятий, направленных на подбор, обучение и адаптацию кадров органов финансово-кредитного контроля.

В рамках данной меры необходимо постоянно проводить обучение сотрудников банка, своевременно обновлять должностные инструкции, а также осуществлять контроль за их соблюдением. Разумеется, технические средства решают большую часть проблем в борьбе с банковским мошенничеством, однако польза от хорошо обученного сотрудника в офисе банка является неоценимой. Также необходимо усилить контроль со стороны кредитных организаций и установить ответственность за полное и точное отражение сотрудниками в документах всех данных, необходимых для получения кредита и банковских карт. А для качественной проверки сведений необходимых для выдачи кредитов и банковских карт, следует обеспечить доступ работников банков к соответствующим компьютерным базам данных правоохранительных органов.

Одним из факторов совершения мошенничеств в банковской сфере является «утечка» персональных данных клиентов банков [6; 7, с. 187–235] (в том числе совершенных бывшими банковскими сотрудниками), поэтому необходимо установить ответственность за подобные деяния. Так, согласно ФЗ от 27 июля 2006 г. № 152-ФЗ, защита прав субъекта персональных данных осуществляется только по жалобе лица, чьи данные были разглашены[2]. Поэтому пока не будет установлена ответственность непосредственно за утечки, с этой проблемой справиться не получится.

В ходе встречи с членами Совета по правам человека 7 декабря 2022 г. Президент РФ выступил с инициативой ужесточить ответственность за нарушения в сфере защиты персональных данных. Он отметил, что лица, злоупотребляющие украденными данными, должны понимать, что используют информацию, полученную незаконным путем[3].

В этой связи необходимо определить порядок расследования внутренних хищений банковских данных и провести своего рода показательные процессы по делам виновных лиц в массовых «утечках» в трудовых коллективах банков.

Кроме того, необходимо остановить бесконтрольный сбор данных, их передачу и использование сверх заявленных целей. Нужна унификация пользовательских соглашений операторов персональных данных. Так, следует разработать хартию этики использования персональных данных. Необходимо создать общественную структуру, которая будет заниматься внешним аудитом информационных данных на предмет легального использования. Информационная безопасность должна быть основой всех программ и информационных систем, касающихся банковских данных, поэтому необходимо проводить постоянный аудит их защищенности.

Следует расширить полномочия ведомств, осуществляющих борьбу с «утечками». В частности, Роскомнадзор необходимо наделить правом инструментального контроля потоков данных и условий их хранения и защиты, а Банк России и МВД России — более широкими полномочиями по внесудебной блокировке счетов и номеров мошенников.

Государство пытается устранить данную проблему, в частности в Федеральный закон № 152-ФЗ внесены изменения, согласно которым, оператор больше не вправе осуществлять сбор персональных данных без уведомления уполномоченного органа. С 1 сентября 2022 г. юридические лица и индивидуальные предприниматели до начала обработки персональных данных, обязаны сообщить в Роскомнадзор о том, что намерены их обрабатывать. Уведомление необходимо направить, в случае если для сбора данных используются средства автоматизации (например, компьютер). Если же

[2] О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства РФ. 2006. № 31. Ст. 3451.

[3] Путин предложил ужесточить ответственность за утечку персональных данных // Rengum. URL: https://regnum.ru/news/society/3758585.html.

для сбора используется бумажный носитель, то уведомление не направляется, однако в случае переноса сведения с бумажного носителя в автоматизированную систему, уведомления Роскомнадзора становится обязанностью.

Однако проблема до сих пор осталась не решенной, базы персональных данных все также продолжают «утекать», а мошенники продолжают их активно использовать в своих обманных схемах.

С ростом онлайн технологий кредитования, пользователи могут получить заем дистанционно через систему Онлайн-банк, в этой связи кредитные организации столкнулись с большим разнообразием новых методов «социальной инженерии» [8, с. 72]. Поэтому банки и иные кредитные организации стали уделять повышенное внимание разработке и внедрению новых технических мер зашиты от банковских мошенничеств [9, с. 90–98].

В настоящее время банки для проверки клиентов и сомнительных банковских операций используют антифрод-системы. Такие системы обладают большими преимуществами в борьбе с рассматриваемым преступлением.

На сегодняшний день существуют разные виды «антифрод»-систем, в частности выделяют: отечественные или западные, внутренние или внешние, универсальные или ориентированные.

Чаще всего отечественные банки используют программное обеспечение противодействия мошенничествам «FISAntifraud». С помощью системы проводится автоматическая проверка анкеты заявителя по двум типам мошенничества: внутреннего[4] и внешнего. Система настраивается в зависимости от запросов банка, при этом у банка нет возможности самостоятельно ее редактировать. Основной принцип работы «FISAntifraud» состоит в следующем: потенциальный заемщик заполняет анкету с указанием персональных данных для получения кредита и отправляет на рассмотрение, далее заявка проходит анализ или банковский антифрод путем прогона через специально настроенные сценарии проверок и при выявлении нарушений ей мгновенно присваивается статус «Мошенник», а информация дублируется в реестр мошенников.

Основным недостатком этой системы является то, что опечатки или различное описание одной и той же информации приводят к несрабатыванию или к ложному срабатыванию системы. Кроме того, банк не может самостоятельно изменять структуру системы и ее алгоритмы срабатывания, соответственно для борьбы с новыми схемами мошенничества ее необходимо постоянно обновлять разработчиком. Как правило, для банка могут разработать индивидуальные правила, но этот процесс не быстрый и требует дополнительных материальных вложений.

По нашему мнению, необходимо создать общенациональный сервис, который улучшит и расширит методы борьбы с мошенничествами такого вида.

Банки сами определяют методы противодействия мошенничеству исходя из особенностей продуктов, которые предоставляются клиентам; используемых каналов обслуживания (отделения, интернет-банк, мобильный банк, телефон); а также бюджета, выделяемый для защиты. Например, антифрод-система банка МКБ выявляет попытки снятия денег со счетов клиентов банка. Операторы банка связываются с клиентом для установления законности операции (не находятся ли клиент под давлением преступника)[5]. Газпромбанк для защиты от мошенников среди прочего использует технологию 3D-Secure. Когда клиент, подключенный к сервису «Безопасные платежи в интернете», осуществляет платеж, он вводит реквизиты карты и автоматически перенаправляется на специальную защищенную страницу сайта банка, где подтверждает операцию одноразовым паролем[6]. Подобные инструменты применяются и другими кредитными организациями.

Для повышения эффективности защиты от мошенников банки сотрудничают с мобильными операторами. Так, например, Сбербанк взаимодействует с операторами связи: Tele2, «Мегафоном», МТС и «Билайном». Схема работы проста: банк и сотовый оператор обмениваются черными списками мошеннических номеров. Когда клиенту совершается звонок с такого номера и если у него подключена система определения номера от банка, система уведомляет его о том, что звонит «мошенник». Если же у клиента не подключены дополнительные опции, но при этом ему поступил звонок, после которого он заходит в приложение банка и осу-

[4] Заявки от оформивших кредит под давлением, заполнение анкеты только по копии документов, выявление сговора и работы инсайдеров.

[5] МКБ внедрил специальную систему защиты клиентов-пенсионеров от мошенников // МКБ. URL: https://mkb.ru/news/45561.

[6] 3D Secure // Газпромбанк. URL: https://www.gazprombank.ru/personal/cards/security.

ществляет денежный перевод, высвечивается сообщение: «возможно, Вы переводите деньги мошенникам»[7].

В 2022 г. Тинькофф банк создал платформу безопасности для клиентов банка и Тинькофф Мобайла, которая позволяется защититься от мошенничества, совершаемого методом «социальной инженерии» и иного спама. Основу этой платформы составляет технология «Нейрощит», позволяющая на основе искусственного интеллекта выявлять и пресекать попытки мошенничества во время звонка. «Нейрощит» анализирует информацию, содержащуюся в звуковой волне, преобразует звук в набор данных, которые обрабатываются и сравниваются с накопленными «эталонными» наборами данных мошеннических звонков. Если количество совпадений превышает допустимый порог, разговор маркируется как потенциально опасный и прерывается. Система также анализирует сведения о входящих звонках, объемы и характер трафика, частотность и уникальность[8].

Таким образом, в борьбе с мошенничествами в банковской сфере банкам необходимо обращать внимание на характеристики различных систем противодействия мошенничеству (на их точность и долю ложных срабатываний). Кроме того, следует учитывать, что универсального решения, способного обеспечить полную защиту банка, не существует. Поэтому на каждом участке системы безопасности следует поддерживать адекватный текущему уровню угроз барьер.

В большинстве случаев для защиты от мошеннических посягательств банки используют несколько «антифрод»-систем. При их выборе следует обращать внимание на сложность внедрения и удобство использования, а также на применяемые методы (например, возможности удаленного управления и т.д.). Кроме того, некоторые «антифрод»-системы могут только дополнять основную систему защиты, т.е. решать узкоспециализированную задачу (распознает изображение, речь и т.д.).

Таким образом, ключом к точному обнаружению банковского мошенничества является разработка систем, способных адаптироваться к новым схемам мошенничества. Поэтому обнаружение мошенничества должно развиваться непрерывно, быстрее, чем сами мошенники [10; 11].

Хотелось бы отметить, что уход с рынка западных IT-компаний вынуждает банки искать эффективные системы среди отечественных разработчиков ПО. Поэтому на сегодняшний день возникает вопрос, как в текущих условиях обеспечить информационную безопасность в банках и как перейти к отечественнымIT-решениям в рамках импортозамещения? Разумеется, при переходе на любой новый продукт возникают неудобства, связанные с его дополнительным изучением или непривычным интерфейсом, необходимостью его настройки под запросы банка. Кроме того, придется изменять и процессы противодействия мошенничеству, функционирующие в банке, под новое решение. Возникают и опасения относительно функционала нового продукта, в частности он может оказаться «беднее» старого, а желание организации быстро внедрить его может привести к тому, что в конечном итоге не хватит ресурсов и времени доработать его до качественного продукта. Поэтому эффективным будет внедрение комплекса отечественных систем, причем необходимо это закрепить на законодательном уровне.

В феврале 2023 г. крупные банки объявили о создание общей для всего рынка системы «антифрод»-мониторинга[9]. Единый онлайн-ресурс позволит в автоматическом режиме отслеживать подозрительные звонки и трансакции и предупреждать о них. Банки смогут реагировать на подозрительную активность мошенника мгновенно (в момент, когда он только связался со своей жертвой). Основным недостатком проекта видится его дороговизна и сложность внедрения для менее крупных банков.

Таким образом, банки обладают набором технологических инструментов, позволяющих противодействовать мошенничеству такого вида, однако они малоэффективны в случаи, если мошенничество совершается путем социальной инженерии из-за невозможности контролировать поведение клиента, который сам сообщает мошенникам нужную им информацию.

Отдельно необходимо упомянуть о роли операторов сотовой связи в предупреждении мошенничеств такого вида. Проведенное исследование показало [12, с. 66], что в 2019–2022 гг. мошенничества чаще всего совершались, путем

[7] Фрод // Сбербанк. URL: http://www.sberbank.ru/ru/person/kibrary/vocabulary/frod.

[8] Нейрощит и другие: Тинькофф запустил платформу для максимальной защиты клиентов банка и Мобайла // Тинькофф. URL: https://www.tinkoff.ru/about/news/17082022-tinkoff-launched-platform-for-maximum-protection-bank-and-mobile-customers.

[9] Единым антифродом // Коммерсантъ. URL: https://www.kommersant.ru/doc/5827478.

звонков с использованием функции подмены абонентского номера, что существенно осложняло деятельность правоохранительных органов по изобличению виновных лиц.

Для устранения обозначенных проблем предлагаются следующие пути решения. Во-первых, необходимо запретить прием входящих вызовов с российским АВС-номером из-за рубежа и своевременно уведомлять абонентов о таких вызовах. Во-вторых, следует разработать единые правила идентификации абонентов. В-третьих, создать базу данных телефонных номеров мошенников и установить обязанность для операторов связи блокировать входящие звонки с таких номеров. В-четвертых, в обязательном порядке регулировать бизнес провайдеров IP-телефонии в России.

В последнее время все больше граждан используют в своей повседневной деятельности глобальную сеть Интернет. Эта сеть, как и телевидение, тоже имеет двойной стандарт: с одной стороны, она является средством совершения ряда новых видов мошенничества (приобретение товаров через фиктивные интернет-магазины или интернет-аукционы, махинации с платежными картами и системами и т.п., всегда заканчивается потерей определенных денежных средств жертвы), с другой — обладает мощным профилактическим потенциалом [13, с. 145].

Повышение качества криминологической осведомленности населения о мошенничествах в банковской сфере возможно при помощи современных приложений-мессенджеров, таких как «Viber», «WatsApp» и т.д., которые позволяют отправлять бесплатные сообщения, совершать видео- и голосовые звонки через интернет. Кроме того, для информирования можно использовать приложения банков. Эти не денежно затратные способы позволят эффективно информировать население, повышать социальную активность граждан. Такие меры могут осуществлять работники органов внутренних дел, специально подготовленные члены общественных объединений, а также сотрудники банков.

Для повышения уровня защищенности жертв банковского мошенничества необходимо проводить обучение правилам финансовой грамотности и безопасному использованию ЭСП, оказывать практическую помощь гражданам в технической и физической защите от возможного несанкционированного доступа к их персональным данным. Кроме того, банкам следует проводить тестирование своих клиентов и сотрудников на проверку знаний безопасного использования банковской карты и систем онлайн-банка. Для стимулирования клиентов к качественному тестированию и повышению уровня знаний, банкам следует разработать систему бонусов, например: предоставлять бесплатное обслуживание карты на определенный срок или же кэшбэк на оплату банковской услуги. Работники банка подобное тестирование должны проходить в обязательном порядке.

Указанные меры будут способствовать формированию технически и юридически грамотного поколения граждан, защищенных от набирающих популярность методов «социальной инженерии».

Для предупреждения повторной виктимизации необходимо регламентировать систему «добровольной постановки на учет» потерпевших от мошенничеств в банковской сфере. Такая профилактическая мера будет носить адресный характер, а потенциальная жертва будет заинтересована в получении помощи и лояльнее воспримет попытку контакта со стороны субъектов виктимологической профилактики.

Сами меры выражаются в обучении таких лиц, предоставлении средств индивидуальной технической защиты (специальные экраны, мощные антивирусные утилиты, система подтверждения операции электронным ключом) и др. Кроме того, чтобы не попасться на уловки мошенников, следует периодически проводить мониторинг уже случившихся сливов данных. Например, с помощью соответствующего сервиса в G-mail можно проверить простые, повторяющиеся и похищенные пароли.

Важным моментом предупреждения мошенничеств в банковской сфере является разработка виктимологической памятки для наиболее уязвимых групп населения по безопасному использованию ЭСП, чтобы не стать жертвой банковского мошенника.

В связи с тем что жертвой банковского мошенничества может выступать физическое и юридическое лицо, необходимо это учитывать при построении мер профилактики.

Особенностью виктимности юридических лиц в лице представляющих их сотрудников носит ролевой характер. В свою очередь, проведенное исследование позволило сделать вывод, что на ролевую витимность влияют виды личностной виктимности, поведения представителей юридического лица, способствующего его виктимизации. В частности, работники бан-

ков, для получения премий и бонусов, стремятся выдать как можно больше кредитов, при этом, полноценно не проверяя личность потенциального клиента, а также предоставляемых им документов, необходимых для получения кредита.

В целях снижения виктимности физических лиц, представляющих юридическое лицо в ситуации совершения преступления, необходимо осуществление следующих мероприятий:

– тщательный отбор кандидатов на замещение вакантных должностей;

– проведение ежегодных проверок действующих сотрудников для исключения их преступных связей с мошенниками. Некоторые ученые конкретизируют, каких именно специалистов следует проверять в первую очередь: «… лиц, осуществляющих трудовую деятельность в подразделениях повышенного риска: кредитных отделах, подразделениях залогового обеспечения и др.» [1, с. 150; 14, с. 146];

– усиление ответственности сотрудников кредитной организации за передачу третьим лицам персональных данных клиентов и сведений, составляющих банковскую тайну.

Помимо осуществления мероприятий по проверке и подбору кандидатов на замещение должностей при приеме на работу в банк, также необходимо проводить профилактическую работу с теми лицами, которые по тем или иным причинам были уволены и прекратили там работать.

По мнению некоторых авторов, следует менять подход к восстановительному правосудию в сфере осуществления финансовых услуг [15, с. 86]. Кредитные и подобные им финансовые организации следует рассматривать как профессиональных участников рынка финансовых услуг, а граждан — как изначально «слабую сторону», придерживаясь концепции Закона РФ «О защите прав потребителей», в связи с чем предлагаются ввести понятие «презумпции виновности профессиональных участников рынка финансовых услуг перед гражданами и государством» при непринятии ими мер виктимологической защиты. Тем самым возложить на них гражданско-правовую ответственность за непринятие мер по пресечению дистанционных хищений денег со счетов их клиентов.

Обращает на себя, внимание тот факт, что появление самостоятельных составов, регламентирующих мошенничества в банковской сфере, не улучшило динамику его состояния. По мнению Н. Иванова, «посредством создания специальных составов мошенничества законодатель собственными руками предоставил преступнику возможность выбрать себе наказание» [16, с. 25].

В результате предлагается исключить из уголовного закона специальные составы ст. 159.1 и 159.3 УК РФ, перенеся ответственность за данные преступления в общий состав мошенничества. Предлагаемые изменения будут отражать соответствующую законодательную реакцию на рост числа случаев мошенничества в банковской сфере, а также позволят устранить существующие проблемы квалификации.

Таким образом, проведенное исследование позволило прийти к следующему выводу. Поскольку банковские процессы имеют централизованный, общегосударственный характер, то и меры предупреждения банковского мошенничества могут и должны быть реализованы на всей территории Российской Федерации. Наиболее действенными представляются меры специально-криминологического предупреждения, которые определены при помощи мер, классифицируемых по их содержанию.

Уголовно-правовые меры (совершенствование уголовно-правовой регламентации исследуемых видов мошенничеств).

Технические меры (совершенствование существующих «антифрод»-систем и увеличение сферы их использования; переход на отечественные ПО; совершенствование мер защиты технических устройств, используемых в банковских операциях).

Организационно-управленческие меры (координация взаимодействия служб безопасности банков с органами внутренних дел; подбор, обучение и адаптацию кадров органов финансово-кредитного контроля, проведение предупредительной работы с бывшими сотрудниками банка; обеспечение доступа работников банков к соответствующим базам данных правоохранительных органов для получения своевременной информации, при оформлении кредитов; защиту персональных данных клиентов банков).

Виктимологические меры (профилактическая работа с лицами, обладающими возрастной и ролевой виктимностью; повышение уровня цифровой, финансовой и технической грамотности потенциальных и реальных потерпевших, в целях профилактики рецидива их виктимности; информирование о способах совершения мошенничеств в банковской сфере).

Реализация указанных мер позволит эффективно выявлять и предупреждать банковские мошенничества на всей территории Российской Федерации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Давыдова А.В. Система и меры корпоративного предупреждения преступлений в банках при проведении расчетно-кредитных операций : дис. ... канд. юрид. наук : 12.00.08 / А.В. Давыдова. — Москва, 2013. — 184 с.

2. Иконников Д.Н. Предупреждение хищений в банковской сфере : дис. … канд. юрид. наук : 12.00.08 / Д.Н. Иконников. — Москва, 2012. — 187 с.

3. Эльзессер В.В. Борьба с мошенничеством в банковской сфере : Уголовно-правовой и криминологический аспекты : автореф. дис. … канд. юрид. наук : 12.00.08 / В.В. Эльзессер. — Санкт-Петербург, 2005. — 24 с.

4. Русскевич Е.А. Актуальные проблемы противодействия хищениям в системах дистанционного банковского обслуживания / Е.А. Русскевич. — DOI 10.24412/2072-4098-2022-8251-70-76. — EDN ASHLZG // Имущественные отношения в Российской Федерации. — 2022. — № 8 (251). — С. 70–76.

5. Долганов С.И. Предупреждение корпоративного мошенничества в сфере банковской деятельности : дис. ... канд. юрид. наук : 12.00.08 / С.И. Долганов. — Москва, 2021. — 234 с.

6. Soomro Z. A framework for ID Fraud Prevention Policies in E-tailing Sector / Z. Soomro, M. Shah, J. Thatcher. — DOI https://doi.org/10.1016/j.cose.2021.102403 // Computers & Security. — 2021. — Vol. 109. — P. 16.

7. Ahmed S.R. Preventing Identity Crime: Identity Theft and Identity Fraud / S.R. Ahmed. — BrillNijhoff, 2020. — 766 p. — DOI https://doi.org/10.1163/9789004395978.

8. Христюк А.А. Проблемы уголовно-правовой регламентациии квалификации деяний, совершаемых с использованием электронных средств платежа / А.А. Христюк, Х.А. Асатрян. — DOI 10.17150/1819-0928.2023.24(1).71-79. — EDN PRXJVQ // Академический юридический журнал. — 2023. — Т. 24, № 1. — С. 71–79.

9. Евтушенко И.И. Актуальные направления виктимологической профилактики дистанционных хищений / И.И. Евтушенко. — DOI 10.47475/2411-0590-2022-10909. — EDN CIJBYZ // Виктимология. — 2022. — Т. 9, №1. — С. 90–98.

10. Fraud detection and prevention in e-commerce: A systematic literature review / ViniciusFacco Rodrigues, Lucas MicolPolicarpo, DiórgenesEugênio da Silveira [et al.]. — DOI https://doi.org/10.1016/j.elerap.2022.101207 // Electronic Commerce Research and Applications. — 2022. — Vol. 56. — P. 101207.

11. Nuno Carneiro, Gonçalo Figueira, Miguel Costa A data mining based system for credit-card fraud detection in e-tail / Nuno Carneiro, Gonçalo Figueira, Miguel Costa. — DOI https://doi.org/10.1016/j.dss.2017.01.002 // Decision Support Systems. — 2017. — Vol. 95. — P. 91–101.

12. Репецкая А.Л. Криминологический анализ современного состояния мошенничеств в банковской сфере России / А.Л. Репецкая, Л.А. Петрякова. — DOI 10.24147/1990-5173.2022.19(1).62-72. — EDN PSPQXA // Вестник Омского университета. Серия: Право. — 2022. — Т. 19, № 1. — С. 62–72.

13. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан) :дис. ... канд. юрид. наук / М.С. Гаджиев. — Махачкала, 2004. — 168 с.

14. Ильин И.В. Виктимологическая профилактика экономического мошенничества : дис … канд. юрид. наук / И.В. Ильин. — Нижний Новгород, 2000. — 204 с.

15. Евтушенко И.И. Виктимологическая защита жертв дистанционных хищений / И.И. Евтушенко. — DOI 10.47475/2411-0590-2023-10108. — EDN KFRKFV // Виктимология. — 2023. — Т. 10, №1. — С. 78–88.

16. Иванов Н.Г. Проблемы применения законодательства об ответственности за мошенничество / Н.Г. Иванов. — EDN UNXAHB // Уголовное право. — 2015. — № 5. — С. 25–29.

REFERENCES

1. Davydova A.V. *The System and Measures of Corporate Crime Prevention in Payment Operations. Cand. Diss*. Moscow, 2013. 184 p.

2. Ikonnikov D.N. *Preventing Theft in Banking. Cand. Diss*. Moscow, 2012. 187 p.

3. El'zesser V.V. *Counteracting Fraud in Banking: Criminal Law and Criminological Aspects. Cand. Diss. Thesis*. Saint Petersburg, 2005. 24 p.

4. Russkevich E.A. Actual Problems of Countering Theft in Remote Banking Systems. *Imushchestvennye otnosheniya v Rossiiskoi Federatsii = Property Relations in the Russian Federation*, 2022, no. 8, pp. 70–76. (In Russian). EDN: ASHLZG. DOI: 10.24412/2072-4098-2022-8251-70-76.

5. Dolganov S.I. *Prevention of Corporate Fraud in the Banking Sector. Cand. Diss*. Moscow, 2021. 234 p.

6. Soomro Z., Shah M., Thatcher J. A Framework for ID Fraud Prevention Policies in E-tailing Sector. *Computers & Security*, 2021, vol. 109, pp. 16. DOI: https://doi.org/10.1016/j.cose.2021.102403.

7. Ahmed S.R. *Preventing Identity Crime: Identity Theft and Identity Fraud*. BrillNijhoff, 2020. 766 p. DOI: https://doi.org/10.1163/9789004395978.

8. Khristyuk A.A., Asatryan Kh.A. Problems of Criminal Law Regulation and Quali Cation of Acts Committed Using Electronic Means of Payment. *Akademicheskii yuridicheskii zhurnal = Academic Law Journal*, 2023, vol. 24, no. 1, pp. 71–79. (In Russian). EDN: PRXJVQ. DOI: 10.17150/1819-0928.2023.24(1).71-79.

9. Evtushenko I.I. Current Directions of Victimological Prevention of Remote Theft. *Viktimologiya = Victimology*, 2022, vol. 9, no. 1, pp. 90–98. (In Russian). EDN: CIJBYZ. DOI: 10.47475/2411-0590-2022-10909.

10. ViniciusFacco Rodrigues, Lucas MicolPolicarpo, DiórgenesEugênio da Silveira, Rodrigo da Rosa Righi, Cristiano André da Costa [et al.]. Fraud Detection and Prevention in E-Commerce: A Systematic Literature Review. *Electronic Commerce Research and Applications*, 2022, vol. 56, pp. 101207. DOI: https://doi.org/10.1016/j.elerap.2022.101207.

11. NunoCarneiro, GonçaloFigueira, Miguel Costa. A Data Mining Based System for Credit-Card Fraud Detection in E-tail. *Decision Support Systems*, 2017, vol. 95, pp. 91–101. DOI: https://doi.org/10.1016/j.dss.2017.01.002.

12. Repetskaya A.L., Petryakova L.A. Criminological Analysis of the Current State of Fraud in the Banking Sector of Russia. *Vestnik Omskogo universiteta. Seriya: Pravo = Herald of Omsk University. Series: Law*, 2022, vol. 19, no. 1, pp. 62–72. (In Russian). EDN: PSPQXA. DOI: 10.24147/1990-5173.2022.19(1).62-72.

13. Gadzhiev M.S. *Criminological Analysis of Crimes in the Sphere of Computer Information (based on the materials from the Republic of Dagestan). Cand. Diss*. Makhachkala, 2004. 168 p.

14. Il'in I.V. *Victimological Prevention of Economic Fraud. Cand. Diss*. Nizhnii Novgorod, 2000. 204 p.

15. Evtushenko I.I. Victimological Protection Victims of Remote Theft. *Viktimologiya = Victimology*, 2023, vol. 10, no. 1, pp. 78–88. (In Russian). EDN: KFRKFV. DOI: 10.47475/2411-0590-2023-10108.

16. Ivanov N.G. The Problems of Application of Legislation on Liability for Fraud. *Ugolovnoe pravo = Criminal Law*, 2015, no. 5, pp. 25–29. (In Russian). EDN: UNXAHB.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Петрякова Людмила Александровна — преподаватель кафедры уголовного права Иркутского государственного университета, соискатель кафедры уголовного права и криминологии Института юстиции Байкальского государственного университета, г. Иркутск, Российская Федерация; e-mail: poimanowa@mail.ru, https://orcid.org/0000-0003-1416-9977, SPIN-код: 3607-4003, AuthorID РИНЦ: 1028589, ResearcherID: ABC-1156-2021.

ДЛЯ ЦИТИРОВАНИЯ

Петрякова Л.А. Предупреждение мошенничеств в банковской сфере / Л.А. Петрякова. — DOI 10.17150/2500-4255.2023.17(4).383-391. — EDN TIELEE // Всероссийский криминологический журнал. — 2023. — Т. 17, № 4. — С. 383–391.

INFORMATION ABOUT THE AUTHOR

Petryakova, Lyudmila A. — Instructor, Chair of Criminal Law, Irkutsk State University, Ph.D. Researcher, Chair of Criminal Law and Criminology, Law Institute, Baikal State University, Irkutsk, the Russian Federation; e-mail: poimanowa@mail.ru, https://orcid.org/0000-0003-1416-9977, SPIN-Code: 3607-4003, AuthorID RSCI: 1028589, ResearcherID: ABC-1156-2021.

FOR CITATION

Petryakova L.A. Prevention of Fraud in the Banking Sector. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 4, pp. 383–391. (In Russian). EDN: TIELEE. DOI: 110.17150/2500-4255.2023.17(4).383-391.