Научная статья
https://doi.org/10.23672/SAE.2023.85.24.005
УДК 343.98

ОТДЕЛЬНЫЕ ЗАКОНОМЕРНОСТИ ДИСТАНЦИОННЫХ ХИЩЕНИЙ С БАНКОВСКОГО СЧЕТА, СОВЕРШАЕМЫХ ПУТЕМ ОБМАНА ИЛИ ЗЛОУПОТРЕБЛЕНИЯ ДОВЕРИЕМ, И МЕРЫ БОРЬБЫ С НИМИ

Алымов Д.В., Воротникова А.С.
Юго-Западный государственный университет

Аннотация. *Цель. Статья посвящена дистанционным хищениям с банковского счета, когда преступники путем обмана или злоупотребления доверием получают конфиденциальные данные платежных карт и самостоятельно либо опосредованно, через жертву, осуществляют переводы денежных средств с банковских счетов, обращая в свое пользование.*

Задачи. В ходе исследования приводится анализ текущего состояния Интернет-мошенничества; ретроспектива экономических преступлений в целом; предложения по совершенствованию нормативно-правового регулирования, обеспечивающего безопасность банковских переводов; закономерности совершения и отдельные меры борьбы с дистанционными хищениями с банковского счета путем обмана или злоупотребления доверием.

Методы. В процессе работы над исследованием использовались общенаучные методы исследования (наблюдение, описание, индукция, дедукция, анализ, синтез, гипотеза) и частно-научные (сравнительно-правовой, формально-юридический).

Результаты. Выявлены отдельные закономерности совершения дистанционных хищений с банковского счёта путем обмана или злоупотребления доверием. В статье также приводится анализ некоторых мер по выявлению, пресечению, предупреждению преступлений указанной категории, в том числе включающих применение специальных знаний в области науки и техники.

Выводы. Авторы сформулировали современные закономерности совершения Интернет-мошенничеств на основе их количественных показателей и особенностей, а также ретроспективного анализа экономических преступлений в целом. В настоящем исследовании проанализирована эффективность нормативно-правового регулирования банковских правоотношений, а также применение современных достижений специальных знаний и иные меры по выявлению, раскрытию, расследованию, предупреждению рассматриваемых преступлений.

Ключевые слова: *дистанционное хищение; обман и злоупотребление доверием; Интернет-мошенничество; информационно-телекоммуникационные технологии; банковский счет; банковский перевод; экономическое преступление; кибербезопасность; социальная инженерия.*

Благодарности/финансирование: *Работа выполнена в рамках реализации программы развития ФГБОУ ВО «Юго-Западный государственный университет» проекта «Приоритет 2030».*

INDIVIDUAL PATTERNS OF REMOTE THEFT FROM A BANK ACCOUNT COMMITTED BY DECEPTION OR ABUSE OF TRUST, AND MEASURES TO COMBAT THEM

Dmitry V. Alymov, Anna S. Vorotnikova
Southwestern State University

Abstract*. Object. The article is devoted to remote theft from a bank account, when criminals, by deception or abuse of trust, receive confidential payment card data and independently or indirectly, through a victim, transfer funds from bank accounts, turning them into their own use.*

Research objectives. The study provides an analysis of the current state of Internet fraud; a retrospective of economic crimes in general; proposals for improving the regulatory framework that ensures the security of bank transfers; patterns of commission and individual measures to combat remote theft from a bank account by deception or abuse of trust.

Methods. In the process of working on the study, general scientific research methods (observation, description, induction, deduction, analysis, synthesis, hypothesis) and private scientific (comparative legal, formal legal) were used.

Findings. Separate patterns of remote embezzlement from a bank account by deception or abuse of trust have been identified. The article also provides an analysis of some measures to identify, suppress, and prevent crimes of this category, including those involving the use of special knowledge in the field of science and technology.

Conclusions. The authors formulated modern patterns of Internet fraud based on their quantitative indicators and features, as well as a retrospective analysis of economic crimes in general. This study analyzes the effectiveness of regulatory regulation of banking legal relations, as well as the use of modern achievements of special knowledge and other measures to identify, disclose, investigate, and prevent the crimes under consideration.

Keywords: *remote theft; deception and abuse of trust; Internet fraud; information and telecommunication technologies; bank account; bank transfer; economic crime; cybersecurity; social engineering.*

Введение.

В последние годы повсеместно проявляется тенденция информатизации и цифровизации различных сфер жизни: от образования и науки до бизнеса и избирательной системы. Современные достижения научно-технического прогресса в области информатизации и цифровизации призваны обеспечивать быстрое и эффективное решение социально значимых задач, благодаря мобильности и удаленному доступу населения к информации различного рода; однако, зачастую, недобросовестные пользователи используют указанные технологии из корыстной или иной личной заинтересованности [1, с.110]. Экономическая сфера, в этой связи, является наиболее уязвимой, поскольку материальные ресурсы исторически всегда привлекали большое внимание людей, в том числе преступников.

Обсуждение.

В первых источниках права экономические преступления были тождественны имущественным. Объектом таких преступлений являлись частные права (права собственности). Позже, с возникновением отношений, связанных с определенным порядком экономической деятельности, стали появляться новые составы преступлений. Так, например, Уголовному уложению 1903 года были известны мошенничество, подлог, подделку монеты, цен-

ных бумаг и знаков, банкротство, ростовщичество и прочие преступления [2, с.128]. Однако понятия «экономическое преступление» по-прежнему не существовало.

В Советской России 60–70 годов прошлого столетия, в силу политических причин, в уголовном законодательстве отсутствовал термин «экономика», зато имело место определение «хозяйство». Так, УК РСФСР 1960 года предусматривал уголовную ответственность за хозяйственные преступления, относя к ним посягательства на народное хозяйство или его отдельные отрасли [3].

Многие ученые в различные периоды исследования таких преступлений обращали внимание на сложность определения понятия «экономическое преступление». Так А.М. Медведев не предложил своего взгляда на указанную дефиницию – лишь указал объекты посягательства: экономику, права, свободы, потребности и интересы участников экономических отношений, функционирование экономического (хозяйственного) механизма, социальные ценности и блага [4, с. 47].

По мнению В.С. Устинова и С.В. Устиновой, экономические преступления – есть преступления, посягающие на экономику, права и свободы, потребности и интересы участников экономических отношений, нарушающие нормальное функционирование экономического (хозяйственного) механизма и причиняющего этим социальным ценностям и благам материальный ущерб, характеризующиеся экономической мотивацией и прямым умыслом на причинение вреда названным объектам, которые для данного преступления являются основными [5, с. 48].

Современный отечественный законодатель в Уголовном кодексе Российской Федерации (далее, УК РФ) реализовал широкий подход к определению экономических преступлений, объединив в разделе VIII «Преступления в сфере экономики» три вида преступлений:

• против собственности (глава 21);

• в сфере экономической деятельности (глава 22);

• против интересов службы в коммерческих и иных организациях (глава 23).

Между тем, А.П. Кузнецов отмечает некоторые взаимозависимые недостатки отечественного правового регулирования этой области:

1) неоднозначная локализация новых норм УК РФ и их несоответствие реальной криминологической ситуации в стране;

2) отсутствие системности при структурном выделении группы преступлений в сфере экономики с едиными правилам и юридико-техническим подходом;

3) неоднозначные толкования и взгляды на криминализацию – декриминализацию, а также - систематизацию и классификацию преступлений раздела VIII УК РФ [6].

На наш взгляд, под экономическими преступлениями следует понимать преступления в сфере экономической деятельности, предусмотренные главой 22 УК РФ, а именно, ви-

новно совершенные участником (участниками) экономических отношений общественно опасные деяния, которые нарушают установленный порядок экономической деятельности, связанной с производством, обменом, распределением и потреблением материальных благ и услуг в целях обогащения (личных интересах либо интересах третьих лиц) [7, с.106].

В настоящем исследовании наибольший интерес из числа экономических преступлений представляют дистанционные хищения с банковского счета, когда преступники путем обмана или злоупотребления доверием получают конфиденциальные данные платежных карт и самостоятельно либо опосредованно, через жертву, осуществляют переводы денежных средств с банковских счетов, обращая в свое пользование. Как правило, такие преступления совершаются членами организованных преступных формирований, что представляет наибольшую общественную опасность.

На основании статистических данных МВД РФ, за 2022 год было выявлено 81,8% преступлений экономической направленности от общего количества зарегистрированных преступлений. При этом из 111429 преступлений экономической направленности было раскрыто лишь 79229, из 522065 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации – 142384 [8]. А в период с января по июль 2023 года количество мошенничеств с использованием электронных средств платежа уменьшилось на 24,8%. Однако из 73453 преступлений экономической направленности было раскрыто лишь 50984, из 371362 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации – 104466 [9].

Указанные показатели свидетельствуют о частом совершении рассматриваемых преступлений и низком уровне их раскрываемости. Целью настоящего исследования является формулирование отдельных закономерностей совершения дистанционных хищений с банковского счета путем обмана и злоупотреблением доверия, оценка используемых в настоящее время мер защиты от данных преступных посягательств и разработка, предложение отдельных мер по их выявлению, пресечению, предупреждению.

Результаты.

Несмотря на быстрое развитие и совершенствование преступлений, связанных с информационно-телекоммуникационными технологиями, удалось выявить ряд закономерностей, характерных для совершения дистанционных хищений с банковского счета путем обмана и злоупотребления доверием на современном этапе.

Как правило, такие преступления совершаются членами организованных преступных формирований, что представляет наибольшую общественную опасность. Интернет-мошенники владеют приемами социальной инженерии, что позволяет им оказывать существенное влияние на

жертву. Обращаем внимание, что в этом случае важно не допустить либо факт установления контакта между преступником и жертвой, либо техническую возможность злоумышленнику пользоваться, владеть и распоряжаться денежными средствами с банковского счета владельца.

Современные меры кибербезопасности на основе действующей системы антифрод-защиты не способны пресечь дистанционные хищения с банковского счета, совершаемые путем обмана и злоупотребления доверием, тогда как злоумышленники используют достижения социальной инженерии, вынуждая обманным путем жертв «обходить» вышеупомянутые технологии и передавать преступникам персональные данные для доступа к банковским счетам либо переводить им денежные средства собственноручно. Ольга Скоробогатова, первый заместитель председателя Банка России, не исключила такие риски не только в отношении безопасности безналичных средств платежа, но и цифрового рубля: «Социальная инженерия построена на том, что человек сам передает мошенникам свои персональные данные и финансовую информацию. В этом случае, какой бы высокой и крепкой ни была стена криптографической защиты, вы сами, по сути, распахиваете главные ворота» [10].

В целях выявления Интернет - мошенников, Центральный банк Российской Федерации (далее – ЦБ РФ) в течение несколько лет постоянно пополняет базу обращений граждан и реквизитов счетов, куда переводят денежные средства без согласия клиента. Однако до вступления в юридическую силу Федерального закона от 24.07.2023 № 369-ФЗ "О внесении изменений в Федеральный закон "О национальной платежной системе", такой перевод будет считаться добровольным и не подлежит возврату, если жертва совершит его под влиянием технологий социальной инженерии. Новый закон обязует банки возмещать клиентам похищенные средства, в том числе в результате телефонного мошенничества [11]. В случае операции перевода денежных средств на «подозрительный» счет, банк обязан будет заблокировать карту держателя на два дня, чтобы человек смог оценить свои действия. В случае если банк не заблокировал операцию мошенника из базы ЦБ РФ, и клиент на неё пожаловался, банк обязан вернуть деньги в течение 30 дней. К сожалению, этот законопроект не охватывает случаи, когда перевод осуществляется на счет, которого нет в базе ЦБ РФ, а также на, так называемые, «резервные (страховочные)» абонентские номера либо когда деньги снимают в банкомате и вносят на счет злоумышленника.

Иные меры защиты обманутых граждан также не демонстрируют свою эффективность. Так, страховки кредитных организаций редко покрывают сумму похищенного либо вовсе не предусмотрены в случаях применения техник социальной инженерии.

Тем не менее, предпринимаются новые попытки обеспечения кибербезопасности в этой сфере, которые сложно назвать совершенными. Например, банк «Тинькофф» разрабо-

тал сервис «Защитим или вернем деньги», который предусматривает обязательное оформление сим-карты «Тинькофф Мобайл», необходимость сделать этот номер основным и подключить определитель номера в качестве фильтра желательных и нежелательных звонков. В случае если под влиянием мошенника по телефону жертва действительно совершит перевод (или даже передали ему данные карты и сняли деньги в банкомате), а банк заблокирует операцию, деньги вернутся клиенту в течение суток. Однако если система безопасности сервиса предупредила клиента о том, что это мошенник, но держатель карты все равно перевел денежные средства, их не вернут [12].

Наиболее успешной и перспективной мерой безопасности банковских счетов от телефонного мошенничества нам видится применение способа и системы анализа голосовых вызовов на предмет выявления и предотвращения социальной инженерии [13]. Указанное техническое решение относится к области вычислительной техники и предполагает установку на устройства связи, обеспечивая безопасность телефонного разговора. Целью его является выявление мошеннической активности посредством комбинированного анализа аудиопотока и семантики паттерна диалога. Иными словами, в ходе прослушивания телефонного разговора будет выявлено, что лицом, совершившим телефонный звонок, является Интернет-мошенник.

Аналогичное программное обеспечение создано не только для анализа телефонных звонков, но и сообщений в различных электронных коммуникационных системах, таких как электронная почта, мессенджеры, SMS и другие источники [14].

Однако мы предполагаем, что не все граждане готовы будут согласиться на такие меры, ссылаясь на обеспечение права тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, гарантируемое ст. 23 Конституции Российской Федерации (далее – Конституции РФ) [15]. Компромиссным нам видится решение анализировать с помощью указанного технического решения не все входящие вызовы и сообщения, а только те из них, которые не записаны в телефонную книгу технического устройства, если речь идет о мобильной связи и мессенджерах.

Заключение.

В результате проведенного исследования было выявлено значительное количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, к числу которых относятся и дистанционные хищения с банковского счета, совершаемые путем обмана или злоупотребления доверием. Кроме того, критическая доля рассматриваемых преступлений остается нераскрытой.

Также, представляют научную ценность выявленные закономерности совершения Интернет-мошенничеств, поскольку они имеют значение для выявления, пресечения и предупреждения рассматриваемых преступлений.

Авторы выражают надежду, что после вступления в юридическую силу Федерального закона от 24.07.2023 № 369-ФЗ "О внесении изменений в Федеральный закон "О национальной платежной системе" будут созданы условия, обеспечивающие безопасность личных финансов граждан и банковской системы в целом. Однако в целях усиления эффективности мер по выявлению, пресечению и предупреждению случаев Интернет-мошенничества и сохранности денежных средств участников банковских правоотношений предлагается повсеместно внедрить алгоритмы распознавания мошеннических предложений, поступающих во время телефонного звонка и сообщения в различных электронных коммуникационных системах. Чтобы не допустить ограничение конституционных прав и свобод граждан, предлагается компромиссное решение: анализировать не все входящие вызовы и сообщения, а только те из них, которые не записаны в телефонную книгу технического устройства.

Анализ отечественного законодательства, систем безопасности отдельных банков, работ российских ученых позволил выявить преимущества и недостатки применения цифровых технологий при выявлении, пресечении и предупреждении дистанционных хищений с банковского счета, совершенных путем обмана и злоупотребления доверием, а также предложить оптимальные пути решения обнаруженных проблем.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Старостенко Н.И. Социальная инженерия как объект криминалистического изучения // Вестник Казанского юридического института МВД России. 2021. № 1 (43) – С. 109-114.

2. Хрестоматия по истории государства и права России: учеб. пособие /сост. Ю.П. Титов.-2-е изд., перераб. и доп. – М.: ТК Велби, Изд-во Проспект, 2005. – 464 с.

3. Хилюта В.В. Экономические преступления: эволюция уголовно-правового регулирования // Всероссийский криминологический журнал. – 2007. №1-2. URL: https://cyberleninka.ru/article/n/ekonomicheskie-prestupleniya-evolyutsiya-ugolovno-pravovogo-regulirovaniya

4. Медведев А.М. Экономические преступления: понятие и система // Советское государство и право. - М.: Наука, 1992, № 1. – 81 с.

5. Устинов В.С., Устинова С.В. Понятия экономического преступления и экономической преступности // Экономическая безопасность России: политические ориентиры, законодательные приоритеты, практика обеспечения: Вестник Нижегородской академии МВД России. 2002. № 2. – С. 41-49.

6. Кузнецов А. П. Экономическое преступление и экономическая преступность: соотношение понятий // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. №3 (39). URL: https://cyberleninka.ru/article/n/ekonomicheskoe-prestuplenie-i-ekonomicheskaya-prestupnost-sootnoshenie-ponyatiy

7. Воротникова А.С. К вопросу о понятии экономических преступлений: современное состояние // В сборнике: ЮГО-ЗАПАДНЫЙ ЮРИДИЧЕСКИЙ ФОРУМ. сборник научных трудов Юго-Западного юридического форума, посвященного 30-летию юридического факультета Юго-Западного государственного университета. Юго-Западный государственный университет. Курск, 2021. С. 105-109.

8. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2022 года // МВД.РФ URL: https://мвд.рф/reports/item/35396677/

9. Краткая характеристика состояния преступности в Российской Федерации за январь - июль 2023 года // МВД.РФ URL: https://мвд.рф/reports/item/40874008/

10. «Цифровой рубль – это новые возможности для человека и бизнеса»: Плюсы, минусы и перспективы новой формы российской валюты // Комсомольская правда URL: https://www.kp.ru/daily/27535/4801749/

11. Законопроект (Федерального закона от 24.07.2023 № 369-ФЗ "О внесении изменений в Федеральный закон "О национальной платежной системе") http://publication.pravo.gov.ru/Document/View/0001202307240049?index=19

12. Мошенничество, связанное с банковскими операциями, наконец стало получать должное внимание — как со стороны регуляторов, так и со стороны бизнеса. // ТИНЬКОФФ URL: https://www.tinkoff.ru/invest/social/profile/AMMiMi.Bank/0d6f23b9-cbd2-4647-9012-0193532aaaa8/

13. Свидетельство о регистрации СМИ № ФС77-47467 Электронный паспорт ФГИС № ФС77110096 Патент № 2790946 C1 Российская Федерация, МПК G06F 40/30, G10L 15/02. Способ и система анализа голосовых вызовов на предмет выявления и предотвращения социальной инженерии : № 2022103928 : заявл. 16.02.2022 : опубл. 28.02.2023 / И. А. Оболенский, К. Е. Вышегородцев, Д. Н. Губанов, И. В. Богданов ; заявитель Публичное акционерное общество "Сбербанк России".

13. Свидетельство о государственной регистрации программы для ЭВМ № 2022665102 Российская Федерация. Программный комплекс для обнаружения атак социальной инженерии на основе методов анализа естественного языка : № 2022663709 : заявл. 21.07.2022 : опубл. 09.08.2022 / В. А. Частикова, В. Г. Гуляй ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный технологический университет».

14. Конституция Российской Федерации от 12.12.1993 // Официальный интернет-портал правовой информации. - 2020 г. - с изм. и допол. в ред. от 01.07.2020.

Referances:

1. Starostenko N.I. Social engineering as an object of forensic study // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2021. No. 1 (43) – pp. 109-114.

2. Anthology on the history of state and law of Russia: studies. manual /comp. Yu.P. Titov.-2nd ed., reprint. and additional. – M.: TK Velbi, Publishing house Prospect, 2005. – 464 p.

3. Khilyuta V. V. Economic crimes: the evolution of criminal law regulation // All-Russian Criminological Journal. 2007. No.1-2. URL: https://cyberleninka.ru/article/n/ekonomicheskie-prestupleniya-evolyutsiya-ugolovno-pravovogo-regulirovaniya

4. Medvedev A.M. Economic crimes: concept and system // Soviet state and law. - Moscow: Nauka, 1992, No. 1. – 81 p.

5. Ustinov V.S., Ustinova S.V. Concepts of economic crime and economic crime // Economic security of Russia: political guidelines, legislative priorities, practice of ensuring: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2002. No. 2. – pp. 41-49.

6. Kuznetsov A. P. Economic crime and economic crime: correlation of concepts // Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2017. No.3 (39). URL: https://cyberleninka.ru/article/n/ekonomicheskoe-prestuplenie-i-ekonomicheskaya-prestupnost-sootnoshenie-ponyatiy

7. Vorotnikova A.S. On the question of the concept of economic crimes: the current state // In the collection: SOUTH-WESTERN LEGAL FORUM. collection of scientific papers of the Southwest Legal Forum dedicated to the 30th anniversary of the Faculty of Law of Southwest State University. Southwest State University. Kursk, 2021. pp. 105-109.

8. Brief description of the state of crime in the Russian Federation for January - December 2022 // Ministry of Internal Affairs.RF URL: https://мвд.рф/reports/item/35396677/

9. Brief description of the state of crime in the Russian Federation for January - July 2023 // Ministry of Internal Affairs.RF URL: https://мвд.рф/reports/item/40874008/

10. "The digital ruble is new opportunities for people and businesses": Pros, cons and prospects of a new form of the Russian currency // Komsomolskaya Pravda URL: https://www.kp.ru/daily/27535/4801749 /

11. Draft Law (Federal Law No. 369-FZ of 07/24/2023 "On Amendments to the Federal Law "On the National Payment System") http://publication.pravo.gov.ru/Document/View/0001202307240049?index=19

12. Fraud related to banking operations has finally begun to receive due attention — both from regulators and from businesses. // TINKOFF URL: https://www.tinkoff.ru/invest/social/profile/AMMiMi.Bank/0d6f23b9-cbd2-4647-9012-0193532aaaa8/

13. Certificate of Registration of Mass media No. FS77-47467 Electronic passport of FGIS No. FS77110096 Patent no. 2790946 C1 Russian Federation, IPC G06F 40/30, G10L 15/02. Method and system of analysis of voice calls for the detection and prevention of social engineering : No. 2022103928 : application. 02/16/2022 : publ. 02/28/2023 / I. A. Obolensky, K. E. Vyshegorodtsev, D. N. Gubanov, I. V. Bogdanov ; applicant Public Joint Stock Company "Sberbank of Russia".

14. Certificate of state registration of the computer program No. 2022665102 Russian Federation. Software package for detecting social engineering attacks based on natural language analysis methods : No. 2022663709 : application 21.07.2022 : publ. 09.08.2022 / V. A. Chastikova, V. G. Gulyai ; applicant Federal State Budgetary Educational Institution of Higher Education "Kuban State Technological University".

15. Constitution of the Russian Federation of 12.12.1993 // Official Internet portal of legal information. - 2020 - with amendments and additions. in ed. from 01.07.2020.

Информация об авторах:

Алымов Дмитрий Владимирович, кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики, «Юго-Западный государственный университет», sledczy@list.ru

Воротникова Анна Сергеевна, аспирантка кафедры уголовного процесса и криминалистики, «Юго-Западный государственный университет», Курск, Российская Федерация, seamni46@mail.ru

Dmitry V. Alymov, Candidate of Law, Associate Professor of the Department of Criminal Procedure and Criminalistics, Southwestern State University, Kursk, Russian Federation

Anna S. Vorotnikova, Post-graduate Student of the Department of Criminal Procedure and Criminalistics; Southwest State University; Kursk, Russian Federation