Научная статья
УДК 343.9
EDN EFDPXZ
DOI 10.17150/2500-4255.2024.18(4).341-348

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО: СОВРЕМЕННЫЕ УГРОЗЫ И ВЫЗОВЫ

Е.В. Демидова-Петрова[1], Е.В. Зотина[2]
[1] Казанский юридический институт (филиал) Университета прокуратуры Российской Федерации, г. Казань, Российская Федерация
[2] Казанский юридический институт МВД России, г. Казань, Российская Федерация

Информация о статье

Дата поступления
19 июня 2024 г.

Дата принятия в печать
27 сентября 2024 г.

Дата онлайн-размещения
15 октября 2024 г.

Ключевые слова

Дистанционное мошенничество; социальная инженерия; информационная безопасность; криминологическая угроза; нейросеть

Аннотация. Повсеместное внедрение информационно-телекоммуникационных технологий во все сферы общественной жизни спровоцировало рост цифровой, или высокотехнологичной, преступности. Статистические данные о преступности свидетельствуют, что количество преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, ежегодно увеличивается, что обусловливает актуальность избранной темы, свидетельствует о неблагоприятном криминологическом прогнозе и требует разработки действенных мер предупреждения, направленных на устранение и минимизацию детерминант данных противоправных деяний. В статье рассматривается одно из преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, — телефонное мошенничество. Указывается на наличие терминологической неопределенности в юридическом научном дискурсе в отношении рассматриваемого термина; приведена криминологическая интерпретация существующих толкований. По мнению авторов, телефонное мошенничество предполагает целенаправленное воздействие преступника на эмоционально-волевую сторону жертвы посредством использования приемов социальной инженерии как совокупности психологических и речевых способов манипулирования потенциальной жертвой в целях достижения преступной цели. Особое внимание уделено описанию приемов социальной инженерии, применяемых при совершении данного противоправного деяния. Установлено, что наиболее часто используются два приема социальной инженерии — алгоритм (претекст) и фишинг. Рассматриваются технологии искусственного интеллекта, вовлеченные в преступную мошенническую деятельность; предлагается комплекс мероприятий по общесоциальному, специально-криминологическому, индивидуальному предупреждению телефонного мошенничества с использованием позитивных возможностей нейросети, направленный на минимизацию и устранение криминальных угроз генеративного искусственного интеллекта. Делается вывод о перспективе симбиоза искусственного и естественного интеллекта в целях наиболее эффективного противодействия преступным посягательствам телефонных мошенников; при этом главенствующая роль принадлежит человеческому разуму.

Original article

PHONE FRAUD: MODERN THREATS AND CHALLENGES

Elizaveta V. Demidova-Petrova[1], Elena V. Zotina[2]
[1] Kazan Law Institute (branch) of University of Prosecutor's Office of the Russian Federation, Kazan, the Russian Federation
[2] Kazan Law Institute of the Ministry of Internal Affairs of the Russian Federation, Kazan, the Russian Federation

Article info

Received
2024 June 19

Abstract. Widespread introduction of information-communication technologies in all spheres of public life led to a rise in digital, or hi-tech, crime. Statistical data on crime shows that the number of crimes committed with the use of information-communication technologies is growing year by year, which proves the relevance of this research topic, points to an unfavorable criminological forecast and requires the

ISSN 2500-1442

Accepted
2024 September 27
Available online
2024 October 15

Keywords
Remote fraud; social engineering; information security; criminal threat; neural network

development of effective prevention measures aimed at eliminating and minimizing the determinants of these unlawful actions. The authors examine one of such crimes committed using information-telecommunication technologies — the crime of phone fraud. They discuss the terminological uncertainty regarding the term under consideration in legal research discourse and present a criminological interpretation of the existing definitions. According to the authors, phone fraud presupposes a purposeful influence of the criminal on the emotional-volition sphere of the victim through techniques of social engineering as an aggregate of psychological and linguistic means of manipulating the potential victim in order to achieve the criminal goal. Special attention is paid to describing the techniques of social engineering used in such unlawful actions. It is established that the two most popular techniques are an algorithm (pretext) and phishing. The authors analyze artificial intelligence technologies involved in criminal fraud activities; they present a complex of measures of general social, special criminological, individual prevention of phone fraud by using neural networks, which are aimed at minimizing and eliminating the criminal threats of generative artificial intelligence. The authors draw conclusions regarding the prospects of a symbiosis between artificial and natural intelligence for a most effective counteraction of criminal infringements committed by phone fraudsters, where the leading role is played by the human mind.

Информационная глобализация и цифровизация оказывают существенное влияние на все сферы общественной жизни, что неизбежно способствует и трансформации преступности. Активно развиваются информационно-телекоммуникационные технологии, которые получают активное применение в противоправных целях.

Неслучайно в Стратегии национальной безопасности Российской Федерации отмечено, что быстрое развитие информационно-телекоммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства[1]. Согласно статистическим данным ГИАЦ МВД России, сегодня каждое третье преступление совершается с использованием информационно-телекоммуникационных технологий[2]. Все большее распространение получает криминальное использование технологий искусственного интеллекта, особенно при реализации дистанционных мошеннических действий.

Пандемия коронавирусной инфекции COVID-19 в 2020 г., проведение специальной военной операции послужили катализаторами для преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в том числе мошенничеств, число которых существенно увеличилось — с 237 074 в 2020 г. до 356 079 в 2023-м[3]. В 2023 г. от действий киберпреступников пострадали полмиллиона человек, из которых практически каждый четвертый — пенсионер. В 2024 г. жертвами преступлений с использованием информационно-телекоммуникационных технологий стали более 40 тыс. граждан пожилого возраста. Существенным является размер причиненного ущерба. Суммарно за 2023 г. и четыре месяца 2024 г. он превысил 210 млрд р.[4]

Особое место среди подобных противоправных деяний занимает телефонное мошенничество, представляющее собой организованную форму преступной деятельности, приобретающей массовый характер. Согласно результатам мониторингового опроса россиян, посвященного телефонному мошенничеству и проведенного ВЦИОМ России, в 2023 г. 67 % россиян столкнулись с данным явлением, тогда как в 2021 г. данный показатель составлял 57 %[5].

В юридическом научном дискурсе встречаются такие варианты наименований, как

[1] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 2 июля 2021 г. № 400 // Собрание законодательства РФ. 2021. № 27, ч. 2. Ст. 5351.

[2] Состояние преступности в России за январь — декабрь 2023 года // ГИАЦ МВД России. URL: https://мвд.рф/reports/item/47055751 (дата обращения: 08.04.2024).

[3] Состояние преступности в России за январь — декабрь 2020 года // ГИАЦ МВД России. URL: https://мвд.рф/reports/item/22678184 (дата обращения: 08.04.2024) ; Состояние преступности в России за январь — декабрь 2023 года.

[4] Владимир Колокольцев провел заседание коллегии МВД России, посвященное противодействию IT-преступности. URL: https://mvdmedia.ru/news/official/vladimir-kolokoltsev-provel-zasedanie-kollegii-mvd-rossii-posvyashchennoe-protivodeystviyu-it-prestu (дата обращения: 05.06.2024).

[5] Телефонное мошенничество: мониторинг // ВЦИОМ России. URL: https://wciom.ru/analytical reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-monitoring (дата обращения: 08.04.2024).

«телефонное мошенничество», «мошенничество с использованием средств сотовой связи», «мошенничество с использованием средств мобильной связи», «мошенничество с использованием телекоммуникационного и компьютерного оборудования», «мошенничество с использованием информационно-телекоммуникационных технологий» [1; 2].

Анализ научной литературы по проблеме исследования позволяет сделать вывод, что существуют следующие криминологические трактовки понятия мошенничества с использованием информационно-телекоммуникационных технологий:

1. Телефонное мошенничество, т.е. мошенничество, в результате которого криминальное взаимодействие преступника и жертвы осуществляется с использованием стационарной телефонной связи, мобильных средств сотовой связи. Средство совершения преступления или средство манипуляции — стационарный телефон или мобильный телефон, способ совершения преступления — обман или злоупотребление доверием. Содеянное квалифицируется по ст. 159 Уголовного кодекса Российской Федерации (далее — УК РФ) как общеуголовное мошенничество.

2. Компьютерное мошенничество (или мошенничество с использованием компьютерного оборудования) предусматривает преступные деяния, связанные с неправомерным воздействием на компьютерную инфраструктуру. Квалифицируется по ст. 159^6 УК РФ.

3. Мошенничество с использованием информационно-телекоммуникационных технологий — наиболее емкая формулировка, предполагающая как преступные деяния, связанные с воздействием на потерпевшего при помощи стационарной телефонной или сотовой связи, так и при помощи таких информационно-телекоммуникационных технологий, как сеть Интернет, приложения-мессенджеры и т.п. При этом в случае звонков посредством IP-телефонии, мессенджеров WhatsApp[6], «ВКонтакте» и др. средством манипуляции выступает мобильный телефон. Средство совершения преступления или средство манипуляции — стационарный или мобильный телефон, персональный компьютер и т.п.; способ совершения преступления — обман или злоупотребление доверием. Квалификация осуществляется по ст. 159 УК РФ (общеуголовное мошенничество), и по специальным ст. 159^3, 159^6 УК РФ (мошенничество с использованием электронных средств платежа и мошенничество в сфере компьютерной информации).

Если обратиться к юридико-техническому анализу терминов «телефонное мошенничество» и «мошенничество с использованием информационно-телекоммуникационных технологий», то следует отметить, что данные термины не тождественны друг другу. В словосочетании «телефонное мошенничество» акцент сделан именно на телефоне (стационарном или мобильном) как средстве осуществления дистанционной коммуникации между преступником и его жертвой. Не всякое мошенничество с использованием информационно-телекоммуникационных технологий — это телефонное мошенничество. Например, целенаправленное воздействие программно-аппаратных средств на сервер или персональный компьютер, направленное на незаконное завладение имуществом и квалифицируемое по ст. 159^6 УК РФ, можно определить как мошенничество с использование информационно-телекоммуникационных технологий, но не как телефонное мошенничество. В свою очередь, любое телефонное мошенничество можно именовать мошенничеством с использованием информационно-телекоммуникационных технологий. Таким образом, понятия мошенничества с использованием информационно-телекоммуникационных технологий и телефонного мошенничества соотносятся как общее и частное.

По нашему мнению, телефонное мошенничество — это мошенничество с использованием информационно-телекоммуникационных технологий, предполагающее целенаправленное воздействие преступника на эмоционально-волевую сторону жертвы посредством использования приемов социальной инженерии. Мошеннические действия могут совершаться как с использованием традиционных средств сотовой или стационарной телефонной связи, так и IP-телефонии, предоставляющей преступникам возможность сохранения анонимности.

Преимущественно понятие социальной инженерии рассматривается в научных работах, посвященных информационной безопасности. В контексте информационной безопасности социальная инженерия — это целенаправленное воздействие на человека и манипулирование им в целях получения конфиденциальной информации либо совершение определенных

[6] Продукт компании Meta, запрещенной на территории Российской Федерации.

действий, направленных на незаконное проникновение (путем обмана) в системы обработки, передачи и распространения информации с целью хищения имущества граждан. Например, под социальной инженерией понимается методика несанкционированного доступа к информационным ресурсам, опирающаяся на особенности человеческой психологии, где объектом непосредственного посягательства являются не информационно-телекоммуникационные системы, а люди — носители кодов доступа к информации [3, с. 96]. По мнению других исследователей в области информационной безопасности и защиты информации, «социальная инженерия — это совокупность методов манипуляции действиями человека в целях получения необходимого доступа к информации. Основная цель социальной инженерии — получение доступа к информации, банковским данным, защищенным системам» [4, с. 152]. В связи с этим одной из стратегических задач государства по обеспечению информационной безопасности является формирование безопасной среды оборота достоверной информации, повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования[7]. Специалисты в области кибербезопасности отмечают, что социоинженерные атаки совершаются не только в отношении взрослых граждан, но и несовершеннолетних. По данным, полученным «Лабораторией Касперского», 15 % детей сталкивались с телефонным мошенничеством, еще столько же — с онлайн-мошенничеством, 13 % — со взломом аккаунтов, а 11 % — с заражением устройств вредоносным программным обеспечением[8]. В связи с этим обеспечение информационной безопасности несовершеннолетних — приоритетное направление в сфере развития государственной информационной политики. Изложенное подтверждает Стратегия комплексной безопасности детей в Российской Федерации на период до 2030 г.: «С учетом темпов развития информационных технологий особую актуальность приобретают угрозы безопасности детей в информационном пространстве. Деструктивное воздействие через средства массовой информации, сеть «Интернет» формирует негативную морально-психологическую атмосферу, способствует росту психических заболеваний, разрушает сложившиеся нормы нравственности, провоцирует противоправное поведение, наносит моральный вред, а также вред здоровью»[9].

В изученной нами отечественной криминологической литературе понятию социальной инженерии уделяется недостаточное внимание, что свидетельствует о необходимости изучения этого феномена именно с криминологической позиции, с учетом достижений активно развивающейся цифровой криминологии. Социальная инженерия как эффективное средство управления человеческими ресурсами с течением времени приобрела все большее криминогенное содержание, особенно в связи со стремительным развитием информационно-телекоммуникационных технологий и вовлечением ее в сферу противоправных деяний, направленных против собственности и безопасности информационных технологий. В зарубежной научной периодике термин «социальная инженерия» получает достаточное освещение [5–11].

Профессор В.С. Овчинский вводит понятие психологической атаки, что, по сути, эквивалентно криминальной социальной инженерии. По мнению исследователя, это особый нетехнический способ получения преступником конфиденциальной информации, основанный на коммуникативном взаимодействии между людьми: «В контексте незаконного доступа к данным этот подход понимается как манипуляция людьми с целью получения доступа к компьютерным системам. Психологическая атака обычно очень успешна, потому что самым слабым звеном в компьютерной безопасности часто являются пользователи компьютерных систем. Пример тому — фишинг, который в последнее время стал основным преступлением, совершаемым в киберпространстве» [12, с 76].

Более развернутое определение социальной инженерии предлагает авторский коллектив монографии «Социальная инженерия и

[7] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 2 июля 2021 г. № 400.

[8] Опрос проведен компанией Online Interviewer по заказу «Лаборатории Касперского» в мае — июне 2022 г. в России среди родителей и их детей школьного и дошкольного возраста. Всего опрошено 2008 чел. — взрослых и детей. URL: https://d-economy.ru/news/jeksperty-podvodjat-itogi-uroka-cifry (дата обращения: 19.06.2024).

[9] О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года : Указ Президента РФ от 17 мая 2023 г. № 358 // Собрание законодательства РФ. 2023. № 21. Ст. 3696.

информационная безопасность». Социальная инженерия — это «система способов воздействия и контроля людей, которая побуждает их совершать определенные действия, применяемая в целях получения персональных данных личности, а также иных конфиденциальных сведений для достижения преступного результата» [13, с. 245]. По мнению авторов данной работы, социальная инженерия относится к разработке и применению методов для преднамеренного манипулирования людьми [13, с. 5]. Исследователи также дают свое определение методов социальной инженерии: «совокупность техник, используемых для манипуляции жертвой с целью получения конфиденциальной информации или выполнения ряда действий, которые могут привести к нарушению информационной безопасности» [13, с. 5].

Полагаем, социальная инженерия — это психологическая и речевая манипуляция человеком в целях достижения преступной цели; а приемы социальной инженерии — совокупность не только психологических, но и речевых способов манипуляции жертвой.

В целях выявления наиболее распространенных приемов социальной инженерии, а также определения ее криминогенного потенциала и прогнозирования тенденций дальнейшего развития нами проведен анализ следственно-судебной практики по уголовным делам о мошенничестве, предусмотренном ст. 159 УК РФ[10], а также выполнен контент-анализ сайтов в сети Интернет, содержащих сведения об использовании приемов социальной инженерии при совершении телефонного мошенничества.

В результате установлено, что чаще всего встречаются такие приемы социальной инженерии, как претекст (алгоритм) и фишинг.

Алгоритм (претекст) (от английского *pretexting* — заранее подготовленный текст) — это прием социальной инженерии, когда преступник отрабатывает заранее подготовленный текст (сценарий), целью которого является совершение потенциальной жертвой определенных действий либо получение конфиденциальной информации, необходимых для хищения денежных средств гражданина. Примеры алгоритма: «Родственник попал в беду», «Перевод средств на безопасный счет» и др.

По нашему мнению, наиболее успешная реализация выбранного мошенниками алгоритма зависит от того или иного личностного качества жертвы, служащего основанием (фундаментом) для эффективного манипулирования, либо совокупности ряда виктимогенных факторов, либо вызываемого алгоритмом чувства (эмоции). При этом качество личности может иметь положительную оценку (привязанность к близким, высокое чувство ответственности и т.п.) либо отрицательную (жадность, алчность). Кроме этого, любой алгоритм имеет чувственно-эмоциональную аффективную основу: основная задача манипулятора вызвать у жертвы эмоцию, определенное чувство, с тем чтобы вывести ее из состояния душевного равновесия и лишить способности рационально оценивать происходящее, а также создать искусственный дефицит времени.

Фишинг (от английского *fishing* — рыбачить, выуживать) — прием социальной инженерии, основанный на обмане пользователя при помощи письменной речи с целью получения от него каких-либо конфиденциальных сведений либо побуждения к совершению определенного действия. В настоящее время распространено создание фишинговых поддельных сайтов интернет-магазинов, маркетплейсов, благотворительных организаций и т.п. Потенциальные жертвы, введенные в заблуждение, сами вводят свои конфиденциальные данные в строку авторизации в личном кабинете, в результате преступники получают доступ к платежным инструментам пользователей.

Особую тревогу вызывает то, что в настоящее время отмечаются случаи симбиоза приемов социальной инженерии и технологий искусственного интеллекта при совершении телефонного мошенничества. Согласно определению, представленному в Национальной стратегии развития искусственного интеллекта на период до 2030 г., технологии искусственного интеллекта — это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машин-

[10] Всего изучено 148 приговоров и материалов уголовных дел, рассмотренных судами Приволжского, Уральского, Центрального федеральных округов.

ного обучения), процессы и сервисы по обработке данных и поиску решений[11].

Имеющаяся практика дает основание утверждать, что используется криминогенный инструментарий искусственного интеллекта в виде дипфейков и чат-ботов для реализации преступных сценариев алгоритма (претекста) и рассылки фишинговых писем.

Технология «дипфейк» позволяет моделировать голос и речь человека на основании имеющегося блока записей «образцов» голоса и речи. Подобные образцы могут быть получены в результате несанкционированного доступа к аккаунтам в социальных сетях или чат-коммуникаторам, содержащим голосовые сообщения, либо в результате криминального мониторинга интернет-пространства, где пользователи могут оставить цифровые следы в виде речевых записей. Сегодня существует несколько разновидностей дипфейков: звуковые, фото- и видео дипфейки (сочетающие комбинацию динамического изображения и голоса человека) [14]. Под технологией «дипфейк» принято понимать совокупность методов соединения фото- и видеоизображений, аудиоинформации в поддельное целое с применением генеративно-состязательных нейронных сетей [15]. При этом системе удается настолько максимально точно сгенерировать акустико-артикуляционные речевые признаки, что отличить голос и речь, созданные при помощи технологии дипфейка, от естественных без наличия специальных познаний крайне сложно. Указанное придает алгоритму (претексту), реализованному при помощи искусственного интеллекта, существенный криминогенный потенциал и повышает степень общественной опасности преступного посягательства, поскольку представляется возможным имитировать голос практически любого человека (при наличии достаточной выборки для обучения системы).

Например, может быть реализован вариант алгоритма (претекста), в ходе которого преступник звонит сотруднику организации, используя аудиодипфейк голоса руководителя, и высказывает требование о перечислении денежных средств. Специалисты в области информационной безопасности указывают на достаточно высокую латентность подобных инцидентов, поскольку зафиксированные случаи зачастую не подлежат разглашению и не фиксируются в материалах официальной статистики преступности[12].

Использование технологии «дипфейк» ставит перед правоохранительными органами новые вызовы. В частности, речь идет о создании методики экспертного выявления голосовых дипфейков. Определение того, является ли исследуемый объект продуктом естественной человеческой речевой деятельности либо искусственно созданным, является насущной и требующей научно-методологического разрешения задачей современного прикладного речеведения, в том числе судебного.

Отмечаются случаи рассылки фишинговых писем, сгенерированных при помощи чат-ботов, например ChatGPT. Такие сообщения могут максимально копировать индивидуально-авторский стиль электронного общения, что в результате повышает степень доверия пользователя к сгенерированному тексту. Необходимо отметить следующие криминогенные особенности нейросетевого чат-бота: способность обработки значительного массива текстовых данных; таргетированная атака (*Advanced Persistent Threat*) — возможность проведения атаки на конкретную компанию или конкретного пользователя; высокая степень самообучаемости системы, что минимизирует возможность идентификации пользователем (потенциальной жертвой) ложного скрипта. Алгоритмы чат-бота способны совершенствовать собственные языковые навыки продуцирования речевых сообщений, что в конечном итоге способствует появлению текста, идентичного созданному при помощи естественного языка, а кроме того, имеющего стилистические признаки авторской индивидуальности, что минимизирует возможности их идентификации пользователем как потенциально криминальных и опасных.

Использование технологий искусственного интеллекта при совершении телефонного мошенничества актуализирует вопросы противодействия данному противоправному деянию, направленные на минимизацию и недопущение новых криминальных вызовов и угроз. Требуется «футурологический подход» для про-

[11] Национальная стратегия развития искусственного интеллекта на период до 2030 года : утв. Указом Президента РФ от 10 окт. 2019 г. № 490 // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

[12] Им голос был, он звал успешно. URL: https://www.kommersant.ru/doc/6466833 (дата обращения: 18.06.2024).

гнозирования новых опасностей и построения комплексной системы правового обеспечения информационной безопасности [16].

По нашему мнению, в области противодействия противоправному использованию технологий искусственного интеллекта при совершении телефонного мошенничества следует применять комплекс мероприятий по общесоциальному, специально-криминологическому и индивидуальному предупреждению. При этом технологии искусственного интеллекта могут использоваться с превентивной целью.

Особое внимание в рамках специально-криминологического и индивидуального предупреждения следует уделять использованию технологий искусственного интеллекта, применяемых в целях:

– обеспечения безопасности абонентов сотовой связи: например, разработке и внедрению сотовыми компаниями — операторами сотовой связи собственных систем обеспечения безопасности абонентов (по типу единой платформы верификации телефонных вызовов «Антифрод») на основе технологий искусственного интеллекта; разработке прикладного программного инструментария с использованием нейросети с целью выявления и блокировки спам-звонков, звонков с «подменных» номеров, фишинговых рассылок;

– выявления лиц, склонных к вовлечению в совершение телефонного мошенничества, на основании нейросетевого мониторинга больших данных и интернет-пространства;

– ограничения доступа к интернет-ресурсам, содержащим в открытом доступе сведения об использовании специальных нейролингвистических и психотехнологий, оказывающих влияние на сознание человека.

Однако представляется необходимым сделать важное уточнение: возможности искусственного интеллекта представляют всего лишь инструментарий, призванный облегчить работу с большими данными. Ведущая роль принадлежит человеческому (естественному) интеллекту, т.е. специалисту, который при помощи имеющихся специальных познаний, умений и навыков способен осуществить профессиональную обработку материала, аккумулированного при помощи нейросети.

Таким образом, «идеальная» модель противодействия телефонному мошенничеству как криминальной угрозе XXI в. — интеграция искусственного и естественного (человеческого) интеллекта.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Леваков А.К. Телефонное мошенничество: трудности противодействия / А.К. Леваков. — EDN DCMNMT // Вестник связи. — 2020. — № 12. — С. 15–16.

2. Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей : дис. … канд. юрид. наук : 12.00.08 / А.С. Камко. — Владивосток, 2020. — 228 с.

3. Байрушин Ф.Т. Социальная инженерия — одна из наиболее опасных угроз ИБ предприятий / Ф.Т. Байрушин, Д.Р. Хлестова. — EDN WXDFIX // Символ науки: международный научный журнал. — 2016. — № 10-2. — С. 95–97.

4. Ломакин А.Л. Социальная инженерия как угроза финансовой безопасности личности / А.Л. Ломакин, Е.Ю. Хрусталев, Г.А. Костюрин. — DOI 10.24891/ni.17.1.150. — EDN PLFUZW // Национальные интересы: приоритеты и безопасность. — 2021. — Т. 17, № 1 (394). — С. 150–166.

5. Albladi S.M. User Characteristics That Influence Judgment of Social Engineering Attacks in Social Networks / S.M. Albladi, G.R.S. Weir // Human-Centric Computing and Information Sciences. — 2018. — Vol. 8, no. 5. — P. 1–24.

6. Comprehensive Assessment of Reverse Social Engineering to Understand Social Engineering Attacks / A. Bishnoi, Garv, S. Bishnoi, N. Gupta // Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023). — Tirunelveli, India, 2023. — P. 681–685.

7. Jakobsson M. Understanding Social Engineering Based Scams / M. Jakobsson. — Springer, 2016. — 130 p.

8. Overview of Social Engineering Attacks on Social Networks / K. Chetioui, B. Bah, A.O. Alami, A. Bahnasse // Procedia Computer Science. — 2022. — Vol. 198. — P. 656–661.

9. Social Engineering, Imperfect Human / J. Neumeier, K. Lemaire, A.P. Taburchak, A.L. Zelezinskii // Economic vector. — 2022. — Vol. 29, no. 2. — P. 11–16.

10. Washo A.H. An Interdisciplinary View of Social Engineering: a Call to Action for Research / A.H. Washo // Computers in Human Behavior Reports. — 2021. — Vol. 4, no. 100126. — URL: https://www.sciencedirect.com/science/article/pii/S2451958821000749.

11. Tayouri D. The Human Factor in the Social Media Security — Combining Education and Technology to Reduce Social Engineering Risks and Damages / D. Tayouri // Procedia Manufacturing. — 2015. — Vol. 3. — P. 1096–1100.

12. Овчинский В.С. Криминология цифрового мира / В.С. Овчинский. — Москва : Норма ; Инфра-М, 2018. — 351 с.

13. Социальная инженерия и информационная безопасность : монография / В.П. Сиротин, М.Ю. Архипова, С.В. Куликова [и др.] — Москва : Эдитус, 2023. — 264 с. — EDN QLTHGH.

14. Киселёв А.С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности / А.С. Киселев. — DOI 10.18384/2310-6794-2021-3-54-64. — EDN AHJBNH // Вестник Московского государственного областного университета. Сер.: Юриспруденция. — 2021. — № 3. — С. 54–64.

15. Батоев В.Б. Использование технологий искусственного интеллекта в выявлении видеодипфейков / В.Б. Батоев, Р.С. Юможапов. — EDN SYZWCV // Вестник Краснодарского университета МВД России. — 2023. — № 3 (61). — С. 76–81.

16. Галяшина Е.И. Вредоносная информация и ее новые виды как угроза медиабезопасности / Е.И. Галяшина // Философско-правовые аспекты опасности антиобщественных идеологий : материалы Междунар. науч.-практ. конф. — Екатеринбург, 2023. — С. 45–58.

REFERENCES

1. Levakov A.K. Phone Fraud: Difficulties of Counteraction. *Vestnik svyazi = Bulletin of Communications*, 2020, no. 12, pp. 15–16. (In Russian). EDN: DCMNMT.

2. Kamko A.S. *Prevention of Fraud with the Use of Telecommunication and Computer Networks. Cand. Diss*. Vladivostok, 2020. 228 p.

3. Bairushin F.T., Khlestova D.R. Social Engineering — One of the Key Threats to the Information Security of Companies*Simvol nauki: mezhdunarodnyi nauchnyi zhurnal = Symbol of Science: International Scientific Journal*, 2016, no. 10-2, pp. 95–97. EDN: WXDFIX. (In Russian).

4. Lomakin A.L., Khrustalev E.Yu., Kostyurin G.A. Social Engineering as a Threat to Personal Financial Security. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*, 2021, vol. 17, no. 1, pp. 150–166. (In Russian). EDN: PLFUZW. DOI: 10.24891/ni.17.1.150.

5. Albladi S.M., Weir G.R.S. User Characteristics That Influence Judgment of Social Engineering Attacks in Social Networks. *Human-centric Computing and Information Sciences*, 2018, vol. 8, no. 5, pp. 1–24.

6. Bishnoi A., Garv, Bishnoi S., Gupta N. Comprehensive Assessment of Reverse Social Engineering to Understand Social Engineering Attacks. *Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023)*. Tirunelveli, India, 2023, pp. 681–685.

7. Jakobsson M. *Understanding Social Engineering Based Scams*. Springer, 2016. 130 p.

8. Chetioui K., Bah B., Alami A.O., Bahnasse A. Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, 2022, vol. 198, pp. 656–661.

9. Neumeier J., Lemaire K., Taburchak A.P., Zelezinskii A.L. Social Engineering, Imperfect Human. *Economic Vector*, 2022, vol. 29, no. 2, pp. 11–16.

10. Washo A.H. An Interdisciplinary View of Social Engineering: a Call to Action for Research. *Computers in Human Behavior Reports*. 2021, vol. 4, no. 100126. URL: https://www.sciencedirect.com/science/article/pii/S2451958821000749.

11. Tayouri D. The Human Factor in the Social Media Security — Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing*, 2015, vol. 3, pp. 1096–1100.

12. Ovchinskii V.S. *Criminology of the Digital World.* Moscow, Norma Publ., Infra-M Publ., 2018. 351 p.

13. Sirotin V.P., Arkhipova M.Yu., Kulikova S.V., Voronkova T.N., Nartsissova S.Yu. *Social Engineering and Information Security*. Moscow, Ehditus Publ., 2023. 264 p. EDN: QLTHGH.

14. Kiselev A.S. On The Expansion of Legal Regulation in the Field of Artificial Intelligence: Deepfake as a Threat to National Security. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Yurisprudentsiya = Bulletin of the Moscow Region State University. Series: Jurisprudence*, 2021, no. 3, pp. 54–64. (In Russian). EDN: AHJBNH. DOI: 10.18384/2310-6794-2021-3-54-64.

15. Batoev V.B., Yumozhapov R.S. The Use of Artificial Intelligence Technologies in the Detection of Video Fake. *Vestnik Krasnodarskogo universiteta MVD Rossii = Bulletin of the Krasnodar University of Ministry of Internal Affairs of Russia Bulletin*, 2023, no. 3, pp. 76–81. (In Russian). EDN: SYZWCV.

16. Galyashina E.I. *Harmful Information and its New Types as Threats to Mediasecurity*. Ekaterinburg, 2023, pp. 45–48.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Демидова-Петрова Елизавета Викторовна — директор Казанского юридического института (филиала) Университета прокуратуры Российской Федерации, доктор юридических наук, доцент, заслуженный юрист Республики Татарстан, член-корреспондент Академии наук Республики Татарстан, г. Казань, Российская Федерация; e-mail: kzn.ui.agprf@mail.ru.

Зотина Елена Владимировна — начальник редакционно-издательского отделения Казанского юридического института МВД России, г. Казань, Российская Федерация; e-mail: ezotina@mail.ru.

INFORMATION ABOUT THE AUTHORS

Demidova-Petrova, Elizaveta V. — Head, Kazan Law Institute (branch) of University of Prosecutor's Office of the Russian Federation, Doctor of Law, Ass. Professor, Honored Lawyer of the Republic of Tatarstan, Corresponding Member of the Academy of Sciences of the Republic of Tatarstan, Kazan, the Russian Federation; e-mail: kzn.ui.agprf@mail.ru.

Zotina, Elena V. — Head, Editorial-and-Publishing Office of Kazan Law Institute of the Ministry of Internal Affairs of the Russian Federation, Kazan, the Russian Federation; e-mail: ezotina@mail.ru.

ВКЛАД АВТОРОВ

Все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

CONTRIBUTION OF THE AUTHORS

The authors contributed equally to this article. The authors declare no conflicts of interests.

ДЛЯ ЦИТИРОВАНИЯ

Демидова-Петрова Е.В. Телефонное мошенничество: современные угрозы и вызовы / Е.В. Демидова-Петрова, Е.В. Зотина. — DOI 10.17150/2500-4255.2024.18(4).341-348. — EDN EFDPXZ // Всероссийский криминологический журнал. — 2024. — Т. 18, № 4. — С. 341–348.

FOR CITATION

Demidova-Petrova E.V., Zotina E.V. Phone Fraud: Modern Threats and Challenges. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2024, vol. 18, no. 4, pp. 341–348. (In Russian). EDN: EFDPXZ. DOI: 10.17150/2500-4255.2024.18(4).341-348.