Научная статья
УДК 343.985.7
https://doi.org/10.36511/2078-5356-2023-1-152-159

Понятие и виды методов социальной инженерии, применяемых при совершении преступлений в сфере информационно-телекоммуникационных технологий

Старостенко Нина Игоревна
Краснодарский университет МВД России, Краснодар, Россия, nstarostenko1996@mail.ru

Аннотация. В настоящее время проблемы, связанные с ростом преступности в сфере информационно-телекоммуникационных технологий, приобретают все большую актуальность. Преступники, совершающие хищения в сфере информационно-телекоммуникационных технологий регулярно совершенствуют преступные навыки, применяя в своей деятельности не только современные программные средства, но и методы социальной инженерии — определенные приемы, в результате использования которых потерпевший либо самостоятельно переводит свои денежные средства на счет преступников, либо передает конфиденциальную информацию (например, персональные данные, данные платежных карт, контрольную информацию, пароли), необходимую для получения доступа к счету. В статье выявлены и проанализированы методы социальной инженерии, используемые в преступной деятельности в качестве своеобразных приемов обмана и психологического манипулирования людьми в целях получения неправомерного доступа к конфиденциальной информации или хищения денежных средств. В работе обоснован подход, в соответствии с которым изучение методов социальной инженерии обусловлено необходимостью их исследования относительно тех характеристик, которые могут позволить определить особенности способов подготовки, совершения и сокрытия преступления, выявить локализацию типичных следов преступной деятельности, дать криминалистическую характеристику личности преступника и потерпевшего, определить обстановку совершения преступления. Решение этой задачи позволит не только эффективно раскрывать и расследовать преступления в сфере информационно-телекоммуникационных технологий, но и принимать меры по их профилактике.

Ключевые слова: криминалистика, расследование преступлений, социальная инженерия, киберпреступления, методы социальной инженерии, информационно-телекоммуникационные технологии

Для цитирования: Старостенко Н. И. Понятие и виды методов социальной инженерии, применяемых при совершении преступлений в сфере информационно-телекоммуникационных технологий // Вестник Нижегородской академии МВД России. 2023. № 1 (61). С. 152—159. https://doi.org/10.36511/2078-5356-2023-1-152-159.

Original article

The concept and types of social engineering methods used in the commission of crimes in the field of information and telecommunication technologies

Nina I. Starostenko
Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russian Federation, nstarostenko1996@mail.ru

Abstract. Currently, the problems associated with the growth of crime in the field of information and telecommunication technologies are becoming increasingly important. Criminals who commit theft in the field of information and telecommunication technologies regularly improve their criminal skills, using in their activities not only modern software tools, but also social engineering methods — certain techniques, as a result of which the victim either independently transfers his money to the account of criminals, or transfers confidential information (for example, personal data, payment card data, control information, passwords) necessary to gain access to the account. The article identifies and analyzes the methods of social engineering used in criminal activity as a kind of deception and psychological manipulation of people in order to obtain unauthorized access to confidential information or theft of funds. The paper substantiates the approach, according to which the study of social engineering methods is conditioned by the need to study them in relation to those characteristics that can make it possible to determine the features of the methods of

© Старостенко Н. И., 2023

preparing, committing and concealing a crime, to identify the localization of typical traces of criminal activity, to give a forensic characterization of the identity of the offender and the victim, to determine the context of the crime. The solution of this problem will allow not only to effectively reveal and investigate crimes in the field of information and telecommunication technologies, but also to take measures to prevent them.

Keywords: criminalistics, crime investigation, social engineering, cybercrime, social engineering methods, information and telecommunication technologies

For citation: Starostenko N. I. The concept and types of social engineering methods used in the commission of crimes in the field of information and telecommunication technologies. *Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2023, no. 1 (61), pp. 152—159. (In Russ.). https://doi.org/10.36511/2078-5356-2023-1-152-159.

Широкое распространение технологий дистанционного банковского обслуживания, увеличение количества транзакций, совершаемых клиентами банков дистанционно через удаленные каналы связи позволяют злоумышленникам осуществлять преступную деятельность удаленно от жертв, используя при этом компьютерную технику, различные программные средства, средства мобильной связи, сеть «Интернет». К превалирующему большинству указанных преступлений относятся хищения, совершенные с применением информационно-телекоммуникационных технологий [1]. Вместе с тем преступники, совершающие данные преступления, регулярно совершенствуют преступные навыки, применяя в своей деятельности не только современные программные средства, но и методы социальной инженерии, в результате использования которых владелец счета либо самостоятельно переводит свои денежные средства на счет преступников, либо передает конфиденциальную информацию (например, персональные данные, данные платежных карт, контрольную информацию, пароли), необходимую для получения доступа к счету [2].

По данным специалистов Центрального банка России приемы и методы социальной инженерии стали основным инструментом злоумышленников для хищения денежных средств [3]. В статистических данных Федеральной службы государственной статистики Российской Федерации приводятся данные относительно применения социальной инженерии при совершении хищений с использованием информационно-телекоммуникационных технологий. Так, за 2020 год количество случаев применения социальной инженерии в корыстных целях составило 71 718, а в 2021 году — 78 754, за 9 месяцев 2022 года — 50 926 (в том числе 1 127 с использованием фишингового поддельного сайта или ссылки) [4].

Высокая степень общественной опасности указанных противоправных деяний подтверждается спецификой преступлений, совершить которые могут лица, обладающие специальными знаниями в области психологии, использующие при этом технические и программные средства, что приводит к нарушению не только права собственности граждан, но и банковской тайны. Вместе с тем общественную опасность данных преступлений усиливает и специфика способа совершения преступления, обусловленная созданием злоумышленниками специально разработанных алгоритмов и сценариев обмана, рассчитанных на их многократное применение в отношении граждан. Кроме того, совершению преступлений обозначенной категории предшествует длительная и тщательная подготовка, заранее предусматривающая способы сокрытия, включающая ряд трудно доказуемых и сложно выявляемых преступных действий, препятствующих своевременному установлению лиц и фактов представляющих криминалистический интерес.

К сожалению, в настоящее время в криминалистической литературе отсутствует единый подход к пониманию и содержанию методов социальной инженерии, применяемых при совершении преступлений. В специальной литературе, в той или иной степени затрагивающей вопрос о сущности социальной инженерии в преступной деятельности, нет строгой однозначности в ее толковании — почти каждый автор предлагает свой аспект решения.

Во многих источниках, посвященных вопросам информационной безопасности, описаны методы социальной инженерии, используемые в противоправных целях. Данные методы получили такие устойчивые обозначения, как «фишинг», «вишинг», «претекстинг», «троянский конь», «кви про кво», «дорожное яблоко», «шантаж» и другие [5, с. 24—26], [6, с. 133—138]. Сравнительно недавно представленная терминология стала заимствоваться из зарубежных источников и использоваться в научных трудах по уголовно-правовым дисциплинам при

характеристике способов совершения преступлений в сфере информационно-телекоммуникационных технологий. Однако, на наш взгляд, данные представления не дают комплексного криминалистического понимания сущности социальной инженерии и ее признаков при совершении хищений в связи с полным отсутствием конкретики и системности. Кроме того, полагаем неприемлемым в полной мере считать методы социальной инженерии в качестве способов совершения преступления. Такая позиция должна находить свое отражение в источниках, посвященных вопросам информационной безопасности, а для решения криминалистических задач имеется потребность в более комплексном рассмотрении специфики социальной инженерии в преступной деятельности.

Полагаем, данные приемы должны быть подвергнуты криминалистическому изучению и описанию относительно тех характеристик, которые могут позволить определить особенности способов подготовки, совершения и сокрытия преступления, выявить локализацию возможных следов преступной деятельности, дать характеристику личности преступника и потерпевшего, определить обстановку совершения преступления. Решение этой задачи позволит не только эффективно раскрывать и расследовать преступления в сфере информационно-телекоммуникационных технологий, но и прогнозировать развитие такой преступной деятельности, а также упредительно принимать меры по ее профилактике.

В рассматриваемом аспекте особого внимания заслуживает позиция профессора А. Л. Осипенко, согласно которой методы социальной инженерии выражены в предварительном сборе информации об организации (жертве); использовании телефона или электронной почты, так как при этом легче выдавать себя за другое лицо; использовании в разговоре или переписке характерных выражений, упоминание известных фактов в совокупности с вымышленными; создании имиджа лица, имеющего полномочия на доступ к запрашиваемой информации; выведении собеседника из состояния психического равновесия путем запугивания, использования резких и унижающих выражений; упоминании в разговоре важных знакомств и связей для формирования у жертвы состояния тревоги относительно возможных негативных последствий в случае отказа от предоставления запрашиваемой информации; употреблении определенных приемов (лесть, личное обаяние и др.) с целью установления психологического контакта [7, с. 112—114].

Изложенное понимание сущности методов социальной инженерии позволяет предположить о том, что они являются своего рода психологическими приемами, а также образом действий злоумышленника, совершающего преступления.

А. Ю. Головин и Е. В. Головина, рассматривая специфику применения социальной инженерии в механизме преступной деятельности в сфере информационно-телекоммуникационных технологий, выделяют следующие ее методы: 1) сообщение потерпевшему о возникших проблемах финансового характера, 2) представление сотрудником банковской или иной кредитной организации, сотрудником правоохранительных органов, 3) предложение оказать помощь в решении финансовых или имущественных вопросов, 4) побуждение вернуть денежные средства, отправленные «по ошибке», 5) побуждение участвовать в лотереях и «финансовых пирамидах», 6) побуждение оказать финансовую помощь людям, находящихся в трудной жизненной ситуации или в связи с состоянием здоровья сетей [8, с. 3—13]. Согласно позиции авторов, криминалистическое понимание социальной инженерии определяется как элемент механизма преступной деятельности в сфере информационно-телекоммуникационных технологий, поскольку данные методы могут применяться в ходе реализации широкого круга преступлений.

Поддерживая названный тезис, добавим, что методы социальной инженерии, при совершении хищений выступают элементом способа совершения преступления в механизме преступной деятельности, изучение которых позволяет познать единый комплекс действий преступника на этапе подготовки, непосредственного совершения и сокрытия хищения.

В этом аспекте также интересна и точка зрения автора генерального директора компании *"Social-Engineer, LLC"* К. Хэднеги, изучающего проявление социальной инженерии в мошеннических схемах. По его мнению, злоумышленники, совершая мошеннические операции с применением социальной инженерии придерживаются схемы поведения, включающей последовательное выполнение действий: сбор данных из открытых источников (фундаментальная деятельность, являющаяся самым значимым звеном мошеннической схемы); разработка повода для атаки (легенда) (планирование мошеннических действий с учетом полученной информации, определение дополнительных инструментов и реквизитов для реализации задуманного); план

атаки (выбор времени и соучастников для совершения преступления); проведение атаки; отчет, при этом выделяя основные направления мошеннической деятельности с применением социальной инженерии: смс-мошенничество (фишинг), голосовой фишинг, имперсонация (подражание сотрудникам полиции, агентам федеральных служб) [9, с. 38—41].

На наш взгляд, представленные подходы к пониманию методов социальной инженерии, применяемые при совершении преступлений, дают более комплексное представление о их сущности и могут быть приемлемы к нашему исследованию с некоторыми уточнениями.

Анализ судебной и следственной практики позволил выделить основные методы социальной инженерии, применяемые злоумышленниками на этапе подготовки, совершения и сокрытия изучаемых преступлений:

1. Использование конфиденциальной информации о потенциальных жертвах.

Конфиденциальную информацию, используемую преступниками при совершении хищений анализируемого вида, можно разделить на следующие группы. К первой группе можно отнести сведения о конкретном человеке или группе лиц, знания о которых позволяет злоумышленникам эффективно вступать во взаимодействие с жертвой, оказывать на нее психологическое воздействие, а также склонять ее к выполнению определенных действий. Необходимо подчеркнуть, что чем больше злоумышленник получит интересующей информации или конфиденциальных сведений о жертве, тем эффективнее применение методов социальной инженерии в процессе совершения преступления. Ко второй группе следует отнести банковские сведения, полученные благодаря использованию методов социальной инженерии и необходимые для хищения чужого имущества.

Например, Д., обвиняемый в совершении преступлений, предусмотренных пунктом «г» части 3 статьи 158 УК РФ, находясь в ФКУ СИЗО-1 ГУФСИН России, расположенном по адресу: <адрес>, используя имеющиеся у него в пользовании средства сотовой связи, посредством сети «Интернет» приискал информацию о клиентах ПАО «ФИО24», а именно: данные личности клиента, дату рождения и абонентский номер, для совершения хищений денежных средств у граждан [10].

Следовательно, информация, относящаяся к первой группе, может собираться как в открытых источниках сети «Интернет», например в социальных сетях (Ф.И.О., абонентский номер телефона, фотографии, идентифицирующие пользователя, его семейное положение, хобби и др.), так и при помощи получения несанкционированного доступа к персональным / банковским сведениям жертв.

Кроме того, отмечаются случаи использования при подготовке к совершению анализируемых хищений программ искусственного интеллекта, которые способны анализировать необходимую информацию и интерпретировать ее для выполнения мошеннических задач. Так, в отчете "*Social Engineering. Blurring reality and fake*" компании "CyberCube" (международная аналитическая компания по страхованию от киберпреступлений) исследователи подробно рассматривают данную проблематику и выделяют тенденцию применения при совершении хищений с использованием социальной инженерии приема «Масштабного социального профилирования» (*Social profiling at scale*). Технологии искусственного интеллекта могут создавать психофизиологические профили лица. В таких профилях, как правило, собирается информация о семье, детях, предпочтениях и хобби, посещаемых местах и заказах [11, с. 63—70]. Таким образом, злоумышленники могут создавать подробный «портрет» жертвы, в котором описывают черты характера, интересы, желания и слабости, что позволяет выстроить механизмы оказания психологического воздействия на жертв.

2. Исполнение определенной роли. Стоит подчеркнуть, что при совершении хищений исследуемого вида преступники исполняют определенные роли (модели поведения), например, сотрудник безопасности банка, кредитный специалист, сотрудник правоохранительных органов, представитель пенсионного фонда или социальной службы, друг, родственник, покупатель, продавец и другие.

Выбор той или иной роли (модели поведения) сопровождается получением более углубленных знаний официально-делового стиля речи, изучением манеры поведения и сферы деятельности конкретного специалиста или сотрудника государственного органа, приобретением знаний об организационной структуре и полномочиях органов государственной власти, общественных организациях и др.

Например, согласно протоколу обыска, проведенного в офисе (колл-центре), созданном для совершения хищений денежных средств у граждан (способ совершения хищений, с применением методов социальной инженерии и средств сотовой связи), обнаружено и изъято:

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2023, no. 1 (61)

заявление на получение карты от имени С., заявление-анкета, заполненное от имени Ф. на выпуск карты; заявление об открытии сберегательного счета и предоставлении потребительского кредита, заполненное от имени И., индивидуальные условия договора потребительского кредита между банком и О.; 4 листа формата А4 с текстом сотрудника банка; 6 листов формата А4 с таблицей, содержащей информацию о расчетах процентной ставки от конкретной суммы денежных средств на определенный срок; заявление-анкета в банке, заявление о предоставлении расчетной (дебетовой) карты в банк, заявление об открытии сберегательного счета и предоставлении потребительского кредита в банк от имени Р. и др. [12].

Данный пример свидетельствует о том, что преступник, совершая преступления, исполнял роль сотрудника банка (кредитного специалиста), придерживаясь которой, он должен был использовать определенный текст, сценарий, изучать документы, которые необходимы специалисту для оказания банковских услуг.

3. Использование при осуществлении преступных действий специально разработанного текста (сценария). Характеризуя данный метод социальной инженерии, стоит отметить, что преступник перед совершением рассматриваемых преступлений осуществляет подготовку текстов-обращений к жертвам для рассылок по смс-сообщениям или электронной почте, разработку алгоритмов обмана и действий по определенному сценарию во время телефонного звонка. Указанные тексты и алгоритмы для результативности применения методов социальной инженерии, как правило, должны обладать аттракцией, включающей создание нужных условий для воздействия на объект [13, с. 33—38].

Так, из материалов уголовного дела следует, что организаторы для совершения хищений предоставляют исполнителям преступных действий рабочее место, выдают мобильные телефоны, *SIM*-карты, а также листы с текстом и данные клиентов, которым необходимо звонить. Указанные листы с информацией являлись «шпаргалкой», текст из которой включал порядок ведения разговора с жертвой и ответы на возможные вопросы. Для убедительности был также подготовлен список определенных документов, которые могут понадобиться для оформления кредита [12].

4. Особая форма подачи информации жертве. Стоит отметить, что тексты (сценарии), подготавливаемые злоумышленниками, «подаются» жертве в особой форме. В этой связи специалистами информационной безопасности Банка России отмечается, что тексты, алгоритмы обманов, а также ответы на вопросы жертвам тщательно разрабатываются психологами, что позволяет преступникам действовать быстро, агрессивно, не давая жертвам одуматься и оценить предпринимаемые действия и шаги [14, с. 20—23]. При этом тексты и алгоритмы подготавливаются таким образом, чтобы они могли помочь вывести человека из спокойного состояния и отключить у него логическое мышление. Для этого они могут запугивать, торопить и оказывать давление или, напротив, стараться заинтересовать и обрадовать внезапной выгодой [15].

Так, из материалов уголовного дела № 1-93/2020 следует, что на протяжении нескольких дней перед тем, как совершать хищения, необходимо пройти стажировку, то есть «подсесть» к кому-либо из уже работающих сотрудников и послушать, о чем они разговаривают с клиентами. Также каждому сотруднику такого колл-центра выдавался лист формата А4, на котором был размещен машинописный текст, который каждый должен был запомнить и выразительно читать при общении с клиентами. При этом основным требованием была грамотная и поставленная речь [12].

5. Создание копий известных интернет-сайтов или применение программных компонентов, позволяющих скрытно и дистанционно оказывать психологическое воздействие на человека (например, программы для изменения голоса, подмены номера телефона, удаленного доступа к мобильному или компьютерному устройству и др.).

В настоящее время злоумышленники предпочитают осуществлять преступную деятельность дистанционно, то есть при отсутствии физического контакта преступника и жертвы (преступник может воздействовать на любой объект сети, находящийся на любом расстоянии от него).

При этом преступники, совершающие хищения, с применением методов социальной инженерии, предпочитают использовать следующие программные средства: программы, позволяющие выполнять подмену абонентского номера при осуществлении телефонных звонков, например "*Call Voice Changer — IntCall*", программы, позволяющие отправить смс-сообщение с подменой абонентского номера отправителя ("*SMSBomba*", "*SmsToo1*", "*SendSMS3*", "*TipTopSMSWin*" и др.), программы для удаленного доступа ("*AnyDesk*" или "*TeamViewer*"),

VPN-сервисы, программные средства "*deepfake*" для создания аудио-, фото- и видеоматериалов с заменой лиц. Такие программы, как правило, находятся в открытом бесплатном доступе в сети «Интернет» и злоумышленник с легкостью может их установить на компьютерное или мобильное устройство и использовать при совершении преступлений. При этом рассмотренные специальные программы заведомо направлены на сокрытие следов хищений, и затрудняют идентификацию злоумышленника по голосу, абонентскому номеру, *IP*-адресу, а также по характеру выполняемых действий при использовании программ удаленного доступа.

Примером использования рассматриваемого метода социальной инженерии могут послужить материалы уголовного дела, из которых следует, что 8 ноября 2019 года по 27 марта 2020 года неустановленное лицо, находясь в неустановленном месте, под предлогом заработка денежных средств на дому, злоупотребив доверием В., убедило его установить на мобильный телефон программу, которая позволила завладеть безналичными денежными средствами В. и перевести их на неустановленный банковский счет, тем самым причинив своими действиями материальный ущерб в особо крупном размере на сумму 5 946 566 рублей [16].

Стоит также подчеркнуть, что преступники, совершающие хищения анализируемого вида, могут обладать умениями по созданию поддельных интернет-сайтов, дублирующих сайты государственных учреждений, известных организаций, порталов государственных услуг (например, «Госуслуги»), форм оплаты сервисов объявлений «Авито», «Юла» и др. Создание подобных сайтов позволяет преступникам убедить жертву перейти по определенной ссылке и ввести данные банковской карты, в том числе *CVV*-код, что способствует хищению денежных средств с банковского счета.

6. Убеждение в необходимости выполнения финансовых операций или сообщения конфиденциальной информации.

Злоумышленник при совершении хищений с применением методов социальной инженерии стремится к тому, чтобы жертва выполнила ряд последовательных действий, связанных с разглашением конфиденциальной информации (банковских сведений) или осуществлением операций по своему банковскому счету, например, произвела перевод денежных средств на безопасный банковский счет через сервис дистанционного банковского обслуживания или банкомат, оформила кредит, совершила покупку, оплатила доставку или услуги государственных учреждений либо передала денежные средства доверенному лицу и др. При этом злоумышленник, принуждая к совершению конкретных действий, создает условия дефицита времени, отпущенного на принятие решения для того, чтобы у жертвы не было возможности верно оценить сложившуюся ситуацию.

Так, в материалах уголовного дела (протокол допроса потерпевшего) № 12016000960002095 представлены показания потерявшего, согласно которым он пояснил, что ему позвонили якобы из кредитно-финансового учреждения и принудили выполнять действия строго по инструкции специалиста для предотвращения мошеннической операции по банковскому счету. Так, в протоколе допроса содержится следующая информация: «… мне сообщили, что для того, чтобы предотвратить мошенническую операцию, нужно следовать строго инструкциям и не отключаться от разговора. Далее я зашел в мобильное приложение «Тинькофф», раздел которого не помню, но который диктовала мне девушка, ввел в данном разделе сумму 75 000 рублей и после чего нажал подтвердить. После этого, открылась следующая страница с *QR*-кодом. Сотрудница банка сообщила, чтобы заблокировать карту нужно получить *QR*-код. Также нужно, чтобы его выдала программа (мобильное приложение). Я нажал кнопку подтвердить, и у меня в галерее фотопленки сохранился скриншот вышеуказанного *QR*-кода. Далее девушка сообщила, что в мобильном приложении "*Whats App*" сейчас поступит сообщение с инструкцией как заблокировать вышеуказанную карту — нужно отправить. Я на номер телефона 8-903… в приложении *"Whats App"* отправил ответное фото с *QR*-кодом…» [17].

В этой связи вполне закономерно говорить о появлении нового вида преступлений, которые обладают своими особенностями и спецификой совершения, анализ которых позволяет сформулировать криминалистическое понимание преступлений, совершенных с использованием методов социальной инженерии.

Таким образом, методы социальной инженерии, применяемые при совершении преступлений (хищений) — это совокупность психологических приемов, технических действий по применению программных средств, технологий в процессе подготовки, непосредственного совершения и сокрытия преступлений, направленных на оказание психологического воздействия на сознание и поведение людей, создание условий, необходимых для дистанционного

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2023, no. 1 (61)

хищения чужого имущества. В понятии важен акцент на то, что применение указанных методов социальной инженерии позволяет преступнику создать такие условия, при которых жертва: 1) самостоятельно выполняет перевод денежных средств на определенный банковский счет, принадлежащий третьим лицам, либо под контролем преступников совершает иные финансовые операции; 2) добровольно предоставляет преступникам удаленный доступ или управление электронным устройством или передает код из смс-сообщений от банка, подтверждающий финансовую операцию, реквизиты банковской карты, в том числе *CVC2 / CVV2* код, логины и пароли от сервиса дистанционного банковского обслуживания, а также иную информацию, необходимую для хищения чужого имущества.

В завершении стоит отметить перспективы дальнейшего изучения методов социальной инженерии во взаимосвязи с элементами криминалистической характеристики преступлений изучаемого вида (личностью преступника, личностью потерпевшего, предметом преступного посягательства, обстановкой и способами совершения преступления, закономерно возникающими типичными следами) и с другой криминалистически значимой информацией. Это позволит не только сформировать криминалистические рекомендации по организации расследования данных преступлений, уточнить организационные и тактические особенности проведения отдельных следственных действий, но и поможет разработать меры криминалистической профилактики, необходимые для упредительного воздействия на данный вид преступности.

Список источников

1. Официальный сайт МВД. Краткая характеристика состояния преступности в Российской Федерации за январь—декабрь 2019 г., 2020 г., 2021 г. URL: https://мвд.рф/reports (дата обращения: 19.01.2022).

2. Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств). URL: https://sozd.duma.gov.ru/bill/186266-7 (дата обращения: 10.11.2021).

3. Официальный сайт Центрального банка России. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. URL: http://www.cbr.ru/analytics/ib/operations_survey_2021/#highlight=социальной%7Синженерии (дата обращения: 10.07.2022).

4. Статистические данные Федеральной службы государственной статистики РФ (форма федерального статистического наблюдения № 280 ИТТ «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий») // О способах совершения преступлений с использованием или применением информационно-телекоммуникационных технологий за 2020, 2021 и 9 мес. 2022 года.

5. Бахтеев Д. В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц // Российское право: образование, практика, наука. 2016. № 3 (93). С. 24—26.

6. Янгаева М. О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. 2021. № 1 (42). С. 133—138. DOI 10.51980/2542-1735_2021_1_133.

7. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. Москва: Юридическое издательство «Норма», 2004. 432 с.

8. Головин А. Ю., Головина Е. В. Социальная инженерия в механизме преступной деятельности в сфере информационно телекоммуникационных технологий // Известия ТулГУ. Экономические и юридические науки. 2021. № 2. С. 3—13.

9. Хэднеги К. Искусство обмана: социальная инженерия в мошеннических схемах. Альпина Паблишер, 2020. 430 с.

10. Приговор Курганского городского суда Курганской области № 1-27/2019 1-885/2018 от 25 февраля 2019 года по делу № 1-27/2019.

11. Желудков М. А. Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // Lex russica (Русский закон). 2021. Т. 74. № 4 (173). С. 63—70. DOI 10.17803/1729-5920.2021.173.4.063-070.

12. Приговор Железнодорожного районного суда г. Барнаула Алтайского края от 28 июля 2020 года по делу № 1-93/2020.

13. Максименко Р. О., Звягинцева П. А. Типовой алгоритм воздействия в социальной инженерии // Интерэкспо Гео-Сибирь. 2019. № 2. С. 33—38.

14. Уваров В. А. Три кита политики финансовой безопасности // Полиция России. 2022. № 5. С. 20—23.

15. Официальный сайт Центрального банка России. Противодействие мошенническим практикам. URL: http://www.cbr.ru/information_security/pmp/#highlight=социальной%7Синженерии (дата обращения: 13.06.2022).

16. Материалы уголовного дела № 12001410033000493, возбужденного 24.09.2020. СО ОМВД России по Сланцевскому району Ленинградской области по признакам, предусмотренным ч. 4 ст. 159 УК РФ.

17. Материалы уголовного дела № 12016000960002095, возбужденного 09.09.2021 СО по РП на ТО отдела полиции № 8 СУ Управления МВД России по г. Ростову-на-Дону по признакам ч. 2 ст. 159 УК РФ.

References

1. Official website of the Ministry of Internal Affairs. Brief description of the state of crime in the Russian Federation for January—December 2019, 2020, 2021. URL: https://mvd.rf/reports (accessed 19.01.2022). (In Russ.)

2. Explanatory note to the draft federal law "On Amending the Criminal Code of the Russian Federation (in terms of strengthening criminal liability for embezzlement of funds from a bank account or electronic money)". URL: https://sozd.duma.gov.ru/bill /186266-7 (accessed 10.11.2021). (In Russ.)

3. Official website of the Central Bank of Russia. Overview of transactions made without the consent of clients of financial institutions in 2021. URL: http://www.cbr.ru/analytics/ib/operations_survey_2021/#highlight=social%7Cengineering (accessed 10.07.2022). (In Russ.)

4. Statistical data of the Federal State Statistics Service of the Russian Federation (form of federal statistical observation no. 280 ITT "Information on crimes committed using information and telecommunication technologies") On the methods of committing crimes using or using information and telecommunication technologies for 2020, 2021 and 9 months 2022. (In Russ.)

5. Bakhteev D. V. On some modern methods of committing fraud in relation to the property of individuals. *Russian law: education, practice, science*, 2016, no. 3 (93), pp. 24—26. (In Russ.)

6. Yangaeva M. O. Social engineering as a way of committing cybercrime. *Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia*, 2021. no. 1 (42), pp. 133—138. (In Russ.)

7. Osipenko A. L. Fighting crime in global computer networks: international experience. Moscow: "Norma" Publ., 2004. 432 p. (In Russ.)

8. Golovin A. Yu., Golovina E.V. Social engineering in the mechanism of criminal activity in the field of information and telecommunication technologies. *Izvestiya TulGU. Economic and legal sciences*, 2021, no. 2, pp. 3—13. (In Russ.)

9. Hadnagi K. Art of deception: social engineering in fraudulent schemes. Alpina Publ., 2020. 430 p. (In Russ.)

10. Judgment of the Kurgan City Court of the Kurgan Region no. 1-27/2019 1-885/2018 of February 25, 2019 in case no. 1-27/2019. (In Russ.)

11. Zheludkov M. A. Justification of the need to adapt the activities of law enforcement agencies to the conditions of digital transformation of the criminal environment. *Lex russica (Russian law)*, 2021, vol. 74, no. 4 (173), pp. 63—70. (In Russ.)

12. Judgment of the Zheleznodorozhny District Court of Barnaul, Altai Territory in case no. 1-93/2020 of July 28, 2020. (In Russ.)

13. Maksimenko R. O., Zvyagintseva P. A. Typical impact algorithm in social engineering. *Interexpo GeoSiberia*, 2019, no. 2, pp. 33—38. (In Russ.)

14. Uvarov V. A. Three pillars of financial security policy. *Police of Russia*, 2022, no. 5, pp. 20—23. (In Russ.)

15. Official website of the Central Bank of Russia. Countering fraudulent practices. URL: http://www.cbr.ru/information_security/pmp/#highlight=social%7Cengineering (accessed: 13.06.2022). (In Russ.)

16. Materials of the criminal case no. 12001410033000493, initiated on 09/24/2020 by the SO MIA of Russia in the Slantsevsky district of the Leningrad region on the grounds provided for in part 4 of art. 159 of the Criminal Code of the Russian Federation. (In Russ.)

17. Materials of the criminal case no. 12016000960002095, initiated on 09.09.2021 by the Investigative Department for the RP on the maintenance of the police department No. 8 of the Investigative Directorate of the Department of the Ministry of Internal Affairs of Russia for the city of Rostov-on-Don on the grounds of part 2 of art. 159 of the Criminal Code of the Russian Federation. (In Russ.)

Статья поступила в редакцию 15.10.2022; одобрена после рецензирования 05.02.2023; принята к публикации 05.03.2023.

The article was submitted 15.10.2022; approved after reviewing 05.02.2023; accepted for publication 05.03.2023