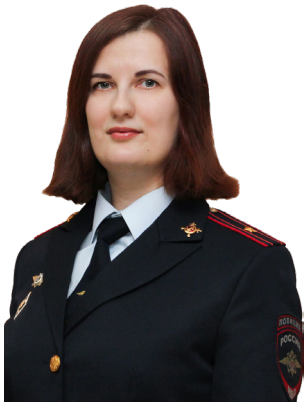
Научная статья
УДК 343.9
DOI: 10.37973/KUI.2022.55.63.012

ПРЕТЕКСТИНГ КАК ПРИЕМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, ИСПОЛЬЗУЕМЫЙ ТЕЛЕФОННЫМИ МОШЕННИКАМИ: КРИМИНОЛОГИЧЕСКИЙ ВЗГЛЯД НА ПРОБЛЕМУ



Елена Владимировна Зотина,
Казанский юридический институт МВД России, Казань, Россия,
ezotina@mail.ru

Аннотация

Введение: в статье рассматриваются криминологические особенности использования преступниками, совершающими мошеннические действия с использованием средств сотовой связи, претекстинга как приема социальной инженерии.

Материалы и методы: эмпирическую основу исследования составили «Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 – 2024 годов», современные научные публикации по проблемам социальной инженерии, официальные сведения МВД по Республике Татарстан о фактах совершения телефонного мошенничества в 2022 году, а также данные проведенного автором социологического опроса. Методология исследования представлена совокупностью общенаучных, частнонаучных и специальных юридических методов, среди которых системно-структурный, логический, конкретно-социологический, лингвистический методы.

Результаты исследования: рассмотрены криминологические аспекты претекстинга, причины, условия его использования, приведены типичные схемы реализации претекстинга в результате совершения телефонного мошенничества, некоторые особенности криминологической характеристики личности преступника. Особое внимание уделено необходимости виктимологической профилактики претекстинга в отношении лиц пенсионного возраста как социально незащищенных граждан и наиболее уязвимой категории населения.

Обсуждение и заключение: автор статьи приходит к выводу, что претекстинг как прием социальной инженерии нуждается в комплексном криминологическом описании с позиций криминологии, социологии, психологии, коммуникативной лингвистики; предлагает возможные направления виктимологической профилактики телефонного мошенничества, совершаемого посредством претекстинга.

Ключевые слова: претекстинг; социальная инженерия; телефонный мошенник; криминологические особенности; виктимологическая профилактика телефонного мошенничества

Для цитирования: Зотина Е.В. Претекстинг как прием социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50). С. 93 – 99. DOI: 10.37973/KUI.2022.55.63.012

Scientific article
UDC 343.9
DOI: 10.37973/KUI.2022.55.63.012

PRETEXTING AS A SOCIAL ENGINEERING TECHNIQUE USED BY TELEPHONE SCAMMERS: A CRIMINOLOGICAL VIEW OF THE PROBLEM

Yelena Vladimirovna Zotina,
the Kazan Law Institute of MIA of Russia, Kazan', Russia, ezotina@mail.ru

Abstract

Introduction: the article discusses the criminological features of the use of pretexting as a social engineering technique by criminals who commit fraudulent actions using cellular communications.

Materials and Methods: the empirical basis of the study were "The main directions of development of the financial market of the Russian Federation for 2022 and the period 2023-2024", modern scientific publications on social engineering, official information of the Ministry of Internal Affairs of the Republic of Tatarstan on the facts of telephone fraud in 2022, as well as data from a sociological survey conducted by the author. The research methodology was represented by a set of general scientific, special scientific and special legal research methods, including system-structural, logical, concrete sociological, linguistic methods.

Results: the criminological aspects of pretexting, the reasons, the conditions of its use were considered, typical schemes for the implementation of pretexting as a result of telephone fraud, some features of the criminological characteristics of the criminal's personality were given. Special attention was paid to the need for victimological prevention of pretexting in relation to persons of retirement age as socially unprotected citizens and the most vulnerable category of the population.

Discussion and Conclusions: the author of the article comes to the conclusion that pretexting as a technique of social engineering needs a comprehensive criminological description from the standpoint of criminology, sociology, psychology, communicative linguistics; suggests measures of victimological prevention of telephone fraud committed through pretexting.

Keywords: pretexting; social engineering; telephone fraudster; criminological features; victimological prevention of telephone fraud

For citation: Zotina E.V. Pretexting as a Social Engineering Technique Used by Telephone Scammers: a Criminological View of the Problem // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2022. Vol. 13. № 4 (50). P. 93 – 99. DOI: 10.37973/KUI.2022.55.63.012

Введение

В настоящее время увеличивается количество мошенничеств, совершаемых посредством использования средств сотовой связи. Мошенничество по телефону становится одним из наиболее простых способов получения несанкционированного доступа к банковской информации граждан.

Согласно данным социологического опроса, проведенного ВЦИОМ России, в первом полугодии 2022 года с телефонным мошенничеством сталкивались большинство россиян – 83% (+7 п.п. к 2021 г.), из них 63% (+6 п.п. к 2021 г.) указали, что им поступали звонки, а 20% получали СМС-сообщения[1]. В 2021 году Россия, по оценке Сбербанка, оказалась в лидерах по телефонному мошенничеству, и ситуация приобрела характер национального бедствия. Станислав Кузнецов, заместитель председателя Сбербанка России, пояснил, что кибермошенники совершают около ста тысяч звонков в день. Девять из десяти владельцев мобильных телефонов сталкивались с мошенниками, а каждый десятый звонок российскому абоненту поступает от преступников[2]. По оценке МВД России, ущерб от телефонного мошенничества в 2021 году составил 45 млрд рублей[3].

В большинстве случаев при совершении преступных посягательств телефонные мошенники

[1] Аналитический обзор ВЦИОМ России. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-i-kak-s-nim-borotsja (дата обращения: 01.12.2022).

[2] Эксперт назвал телефонное мошенничество национальным бедствием // Российская газета. 2021. 7 июля.

[3] Ущерб от телефонного мошенничества с начала года в России составил 45 млрд рублей. URL: https://tass.ru/obschestvo/13194049 (дата обращения: 02.12.2022).

используют такой прием социальной инженерии, как претекстинг, то есть действия по заранее подготовленному сценарию (претексту).

Несмотря на серьезные меры, направленные на повышение информационной грамотности граждан в области противодействия телефонному мошенничеству и предпринимаемые государственными, общественными, финансово-кредитными организациями, проблема продолжает оставаться крайне серьезной и требует дальнейшего научно-теоретического криминологического изучения и выработки действенных мер виктимологической профилактики, способствующих минимизации данного негативного явления.

Материалы и методы

Эмпирическую основу исследования составили стратегический документ, подготовленный Банком России во взаимодействии с Правительством Российской Федерации «Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 – 2024 годов», современные научные публикации по проблемам социальной инженерии, официальные сведения МВД по Республике Татарстан о фактах совершения телефонного мошенничества в 2022 году, а также данные проведенного автором социологического опроса лиц, пострадавших от мошеннических действий по телефону. Методология исследования представлена совокупностью общенаучных, частнонаучных и специальных юридических методов исследования, среди которых системно-структурный, логический, конкретно-социологический, лингвистический методы.

Обзор литературы

Понятие социальной инженерии раскрыто в «Основных направлениях развития финансового рынка Российской Федерации на 2022 год и период 2023 – 2024 годов». Это введение в заблуждение путем обмана или злоупотребления доверием для получения несанкционированного доступа к информации, электронным средствам платежа или побуждения владельцев совершить перевод денежных средств с целью их хищения[1].

В ходе исследования изучены труды отечественных юристов, криминологов, психологов О.П. Грибунова, М.В. Старчикова, М.В. Кузнецова [1, 2], отдельные криминологические аспекты социальной инженерии рассмотрены в коллективной монографии «Проблемы социальной инженерии, информационной и кибербезопасности» (Москва, 2021) [3]. В новейших публикациях по проблемам использования социальной инженерии в рамках совершения дистанционных мошенничеств преимущественно рассматриваются криминалистические особенности, механизм расследования киберпреступлений [4, 5, 6]. Деструктивное влияние мошеннических схем на экономическую безопасность описано в исследовании Л.В. Саниной и др. [7]. Виктимологическим аспектам профилактики кибермошенничества посвящена статья С.А. Стяжкиной [8]. Отсутствие значительного количества фундаментальных монографических исследований, раскрывающих криминологические особенности использования методов и приемов социальной инженерии, в частности претекстинга, свидетельствует о недостаточной научной проработанности проблемы. Кроме того, сами наименования основных приемов социальной инженерии (претекстинг, фишинг (вишинг), «квид про кво», «Троянский конь», «дорожное яблоко») являются весьма условными и сленговыми, требуют легального закрепления и устоявшегося употребления, в том числе и в следственно-судебной практике, на что обращают внимание А.Ю. Головин, Е.В. Головина: «Изучение материалов уголовных дел показывает, что следственная практика нуждается в единой терминологии для описания используемых преступниками приемов социальной инженерии. По факту такие примеры называются в следственно-судебной практике по-разному, например, в процессуальных документах встречается формулировка «психологические приемы и методы наступательной тактики общения»» [4, с. 6].

Результаты исследования

Претекстинг – это мошенническая схема, основанная на методах социальной инженерии[2]. Иными словами, это вид мошеннических действий, совершаемых, как правило, посредством средств сотовой связи, 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. Существует также термин «вишинг» (от английского vishing, Voice phishing). Это еще одна устная разновидность мошенничества, при которой преступники, используя телефонную коммуникацию, стимулируют людей к выдаче

[1] Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 – 2024 годов. Доступ из СПС «КонсультантПлюс» (дата обращения: 02.12.2022).

[2] Энциклопедия Касперского. URL: https://encyclopedia.kaspersky.ru/glossary/pretexting/(дата обращения: 02.12.2022).

конфиденциальной информации или совершению определенных действий. В ряде случаев претекстинг и вишинг используются как синонимы или претекстинг считают разновидностью вишинга. Объединяющим признаком является совершение мошеннических действий посредством телефонной связи, однако претекстинг предполагает более изощренную схему манипулятивного воздействия на жертву, включающую проработку заранее продуманного плана-сценария действий и направленную на установление доверительного эмоционального контакта.

Претекстинг требует от преступника тщательной подготовки к осуществлению личного контакта с жертвой, ему необходимы сведения о ее персональных данных (фамилии, имени, отчестве), личном окружении, семье, потребительских предпочтениях, месте работы (учебы и т.п.). Подобную информацию можно получить в интернет-пространстве в результате изучения профилей жертвы в социальных сетях, онлайн-чатах, а также использования специальных программ, предназначенных для сбора конфиденциальных сведений и поиска личной информации в Интернете. Изучив имеющиеся сведения, преступник может представиться коллегой по работе, работником банковской организации, в которой у гражданина имеется счет, сотрудником правоохранительных органов и т.п. Он может уверенно назвать фамилию, имя, отчество жертвы, осведомлен о ее родственных и дружеских связях, что выступает маркером установления идентичности «свой – чужой» и служит налаживанию доверительного психологического контакта.

Большинство мошеннических атак по телефону совершаются именно посредством претекстинга, что актуализирует необходимость криминологического изучения его детерминант, социальных причин и условий реализации, нравственно-психологических и социально-демографических характеристик личности преступника.

Одной из детерминант рассматриваемого явления являются современные процессы информационной глобализации, активное развитие информационно-телекоммуникационных технологий, обеспечившие возможность поиска и обнаружения персональной информации о потенциальных жертвах, а также технические возможности VPN-сервисов, IP-телефонии, позволяющие осуществлять телефонные звонки от имени официальных организаций, например, финансово-кредитных учреждений. Открытые профили пользователей в социальных сетях, онлайн-чаты предоставляют преступникам практически безграничные возможности поиска идентифицирующей информации о предполагаемой жертве.

Но одних только технических средств недостаточно. Основной причиной достаточно успешного использования претекстинга в качестве приема социальной инженерии являются психологические механизмы человека, когнитивный базис принятия решений. Несмотря на прогрессивное развитие информационно-телекоммуникационных технологий, а также внедрение инновационных криптографических средств защиты информации, человек был и остается основной мишенью. Психологическое манипулирование, выведение человека из состояния душевного равновесия и спокойствия, погружение его в атмосферу стресса, требующего принятия краткосрочных и не контролируемых сознанием мер реагирования, – вот основные задачи телефонного мошенника, использующего претекстинг.

Рассмотрим несколько типичных схем реализации претекстинга. Преступник звонит потенциальной жертве, называя ее фамилию, имя, отчество, представляясь сотрудником банка. При этом он может верно указать наименование банка, в котором у гражданина действительно имеется счет. Далее «сотрудник банка» вежливо просит уделить ему пару минут для уточнения сведений о счете и проверке финансовой безопасности. В результате у жертвы запускается когнитивный механизм, продуцирующий защитные поведенческие реакции. «Сотрудник банка» утверждает, что со счета гражданина неизвестный злоумышленник пытается осуществить несанкционированный перевод денежных средств, и просит уточнить цифровое наименование счета; кроме того, он может даже назвать первые несколько цифр сам. После этого обеспокоенная жертва обозначает оставшиеся цифры самостоятельно, а далее «сотрудник банка», в целях предотвращения нежелательной транзакции и блокировки счета, настоятельно рекомендует передать ему трехзначный CVV-код, указанный на обороте пластиковой карты. В результате он получает полный доступ к денежному счету жертвы. Иногда от жертвы требуется самостоятельно ввести определенную комбинацию цифр или совершить перевод на указанный «сотрудником банка» счет в целях безопасности. *Пример: в начале декабря в полицию обратилась 46-летняя жительница Казани с сообщением о преступлении. Днем на мобильный телефон потерпевшей позвонил неизвестный мужчина. Представившись со-*

трудником одного из банков, он сообщил, что в отношении нее совершаются мошеннические действия и несанкционированные переводы. Звонивший убедил потерпевшую оформить кредит на 350 тысяч рублей и перевести денежные средства на неизвестные счета. После этого потерпевшая прервала еще один финансовый перевод в размере 94 тысяч рублей и обратилась в полицию. В настоящее время по данному факту возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 2. ст.159 Уголовного кодекса Российской Федерации «Мошенничество»[1].

Другая схема телефонного мошенничества с использованием претекстинга. Гражданину, как правило, пенсионного возраста звонит неизвестный, представляясь сотрудником правоохранительных органов. Он сообщает, что его близкий родственник (сын, дочь, внук) попал в ДТП и, в целях уклонения от уголовной ответственности и оказания помощи близкому человеку, необходимо передать «сотруднику» денежные средства. Как правило, последующая передача денежных средств курьеру осуществляется прямо в подъезде дома, где проживает гражданин. Затем курьер переводит денежные средства инициатору мошенничества. *Пример: 3 ноября 2022 года в дежурную часть ОМВД России по Зеленодольскому району Республики Татарстан обратились четыре местных жителя с заявлениями по фактам мошенничества под предлогом «Родственник попал в беду». Установлено, что пенсионерам звонил неизвестный и, представившись сотрудником правоохранительных органов, сообщал о том, что их дочь стала виновницей ДТП, а для оказания медицинской помощи пострадавшему и урегулирования вопросов, связанных с возбуждением уголовного дела, необходимо передать определенную сумму денег. В результате две женщины, 1932 и 1938 года рождения, передали курьерам по 200 тысяч рублей, еще одна 75-летняя пенсионерка и мужчина 1939 года рождения – по 110 тысяч рублей*[2].

На основании изложенного очевидно, что претекстинг предполагает использование преступниками специальных психологических приемов манипулирования, при этом сам преступник необязательно должен иметь соответствующую профессиональную подготовку в области психологии общения, так как сценарий беседы, все коммуникативные стратегии и тактики, используемые при общении, могут быть подготовлены заранее другим лицом.

Кроме того, обратимся к такой важной составляющей криминологического портрета преступника, использующего претекстинг, как речевая подготовка. Проведенный нами социологический опрос лиц, подвергшихся телефонным мошенническим атакам, подтверждает, что крайне важное значение в установлении доверительного контакта имеют просодические характеристики голоса (интонация, тембр, сила голоса), а также высокий уровень речевой (языковой) грамотности преступника – использование им установленных форм речевого этикета, грамотных, полных предложений, терминологической лексики из сферы финансово-кредитных отношений.

В связи с этим полагаем, что, помимо традиционных для криминологической науки социально-демографических и нравственно-психологических признаков криминологической характеристики личности телефонного мошенника, следует дополнительно рассматривать его языковые (речевые) признаки. Это обусловлено спецификой основного канала общения преступника и жертвы – устного общения по телефону. В данном случае в механизм реализации преступного поведения включаются паралингвистические и экстралингвистические средства общения, используемые субъектом преступления сознательно, с манипулятивной целью и направленные на достижение результата – завладение денежными средствами граждан при помощи обмана.

Приведенный выше пример реализации мошеннической схемы «Оказание помощи родственнику, попавшему в ДТП» наглядно демонстрирует, насколько уязвимыми оказываются перед телефонными мошенниками лица пенсионного возраста. В связи с этим обратимся к такой важной криминологической категории, как предупреждение телефонного мошенничества в отношении пенсионеров.

Согласно статистическим данным о состоянии преступности в стране за первые 7 месяцев 2021 года, опубликованным Генеральной прокуратурой Российской Федерации, в 39 200 случаях от действий киберпреступников пострадали российские пенсионеры[3]. С.А. Стяжкина справедливо отмечает, что «самыми незащищенными группами по-прежнему остаются пенсионеры и

[1] Официальный сайт МВД по Республике Татарстан. URL: https://16.мвд.рф/ (дата обращения: 09.12.2022).

[2] Там же.

[3] О состоянии преступности в России за январь-июль 2021 года: сборник Генпрокуратуры России. URL: http://crimestat.ru/analytics (дата обращения: 02.12.2022).

пожилые люди. Современные реалии заставляют их использовать информационные ресурсы, но, к сожалению, у большинства пожилых людей отсутствуют даже самые элементарные навыки работы с компьютерами и информационными системами» [8, с. 550]. И это действительно так. Уровень информационной грамотности пенсионеров, степень их правового информирования, способность защитить персональную информацию в Интернете и оказывать эффективное противодействие дистанционным мошенникам оказываются недостаточными, при этом цифровые следы, оставляемые лицами пенсионного возраста при посещении сайтов интернет-магазинов, использование незащищенного протокола передачи данных, открытая информация в социальных сетях предоставляют телефонным мошенникам существенный кримининогенный потенциал для сбора информации и выявления действенных рычагов психологического воздействия. В связи с этим полагаем, что общая и специальная криминологическая профилактика телефонного мошенничества в отношении лиц пенсионного возраста должна быть направлена в первую очередь на повышение уровня их информационной грамотности, информирование о возможных мошеннических схемах.

Обсуждение и заключение

Вышеизложенное позволяет сформулировать ряд выводов.

Информационная глобализация, внедрение цифровых систем во многие сферы жизнедеятельности человека обусловили возникновение и развитие разных видов дистанционных мошеннических действий с использованием приемов и методов социальной инженерии. Претекстинг как вид мошеннических действий с использованием средств сотовой связи имеет ряд специфических криминологических особенностей, к числу которых следует отнести особо тщательную подготовку, направленную на сбор персональной информации о жертве с целью установления доверительных отношений, использование специальных психологических манипулятивных приемов, элементов экстралингвистического и паралингвистического воздействия на жертву. На основании этого при исследовании причин, условий, механизма формирования преступного поведения, описании криминологической характеристики личности мошенника необходимо использовать междисциплинарные научные связи в области криминологии, психологии, социологии и лингвистической науки.

Виктимологическая профилактика телефонного мошенничества, совершаемого посредством претекстинга, прежде всего, должна осуществляться в отношении лиц пенсионного возраста как социально незащищенной и наиболее уязвимой категории населения и реализовываться комплексно всеми субъектами общей и специальной криминологической профилактики: федеральными органами исполнительной власти, в том числе МВД России, органами прокуратуры, органами государственной власти субъектов Российской Федерации, государственными, общественными и частными структурами, содействующими выполнению правоохранительных задач. Основная цель – повышение уровня информационной (цифровой) грамотности населения, информирование о существующих мошеннических схемах, обучение навыкам психологической устойчивости к техникам манипулирования. При этом отметим, что при реализации профилактических мер необходимо учитывать геронтологические особенности лиц пенсионного возраста; передаваемая им информация должна быть соответствующим образом подготовлена и адаптирована.

СПИСОК ИСТОЧНИКОВ

1. Грибунов О.П., Старчиков М.В. Расследование преступлений в сфере компьютерной информации и высоких технологий. Москва: ДГСК МВД России, 2017. 159 с.
2. Кузнецов М.В. Социальная инженерия и социальные хакеры. Санкт-Петербург: БХВ-ресурс, 2007. 368 с.
3. Нарциссова С.Ю., Куликова С.В., Воронкова Т.Н., Фомина А.С., Архипова М.Ю., Сиротин В.П. Проблемы социальной инженерии, информационной и кибербезопасности: монография. Москва: Инфра-М, 2021. 328 с.
4. Головин А.Ю., Головина Е.В. Социальная инженерия в механизме преступной деятельности в сфере информационно-телекоммуникационных технологий // Известия Тульского государственного университета. Экономические и юридические науки. 2021. № 2. С. 3 – 13.
5. Старостенко Н.И. Социальная инженерия как объект криминалистического изучения // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 1. С. 109-114. DOI: 10.37973/KUI.2021.45.18.017.

6. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России.2021. № 1 (42). С. 133-138.
7. Санина Л.В., Чепинога О.А., Ржепка Э.А., Палкин О.Ю. Деструктивная социальная инженерия как угроза экономической безопасности: масштабы явления и меры предотвращения // Baikal Research Journal. 2021. Т. 12, № 2. DOI: 10.17150/2411-6262.2021.12(2).14
8. Стяжкина С.А. Виктимологическая профилактика кибермошенничества // Вестник Удмуртского университета. Серия «Экономика и право». 2022. Т. 32, № 3. С. 546 – 552.

REFERENCES

1. Gribunov O.P., Starchikov M.V. Rassledovanie prestuplenij v sfere komp'yuternoj informacii i vysokih tekhnologij. Moskva: DGSK MVD Rossii, 2017. 159 s.
2. Kuznecov M.V. Social'naya inzheneriya i social'nye hakery. Sankt-Peterburg: BHV-resurs, 2007. 368 s.
3. Narcissova S.YU., Kulikova S.V., Voronkova T.N., Fomina A.S., Arhipova M.YU., Sirotin V.P. Problemy social'noj inzhenerii, informacionnoj i kiberbezopasnosti: monografiya. Moskva: Infra-M, 2021. 328 s.
4. Golovin A.YU., Golovina E.V. Social'naya inzheneriya v mekhanizme prestupnoj deyatel'nosti v sfere informacionno-telekommunikacionnyh tekhnologij // Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki. 2021. № 2. S. 3 – 13.
5. Starostenko N.I. Social'naya inzheneriya kak ob"ekt kriminalisticheskogo izucheniya // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2021. T. 12, № 1. S. 109-114. DOI: 10.37973/KUI.2021.45.18.017.
6. YAngaeva M.O. Social'naya inzheneriya kak sposob sovershenija kiberprestuplenij // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii.2021. № 1 (42). S.133-138.
7. Sanina L.V., CHepinoga O.A., Rzhepka E.A., Palkin O.YU. Destruktivnaya social'naya inzheneriya kak ugroza ekonomicheskoj bezopasnosti: masshtaby yavleniya i mery predotvrashcheniya // Baikal Research Journal. 2021. T. 12, № 2. DOI: 10.17150/2411-6262.2021.12(2).14
8. Styazhkina S.A. Viktimologicheskaya profilaktika kibermoshennichestva // Vestnik Udmurtskogo universiteta. Seriya «Ekonomika i pravo». 2022. T. 32, № 3. S. 546 – 552.

Информация об авторе:
Зотина Елена Владимировна, начальник редакционно-издательского отделения Казанского юридического института МВД России, ezotina@mail.ru

Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Zotina Yelena Vladimirovna, head of the Editorial and Publishing Department of the Kazan Law Institute of MIA of Russia, ezotina@mail.ru

The author has read and approved the final version of the manuscript.

Статья получена: 11.11.2022.
Статья принята к публикации: 21.12.2022.
Статья опубликована онлайн: 26.12.2022.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.