



Научная статья

УДК 159.99:343.1

<https://doi.org/10.24412/2073-0454-2023-7-289-295>

EDN: <https://elibrary.ru/rbrdzo>

NIION: 2003-0059-7/23-935

MOSURED: 77/27-003-2023-07-134

Необходимость применения комплексного подхода в противодействии телефонному мошенничеству

Любовь Николаевна Костина¹, Владимир Владимирович Гончар²

^{1,2} Московский университет МВД России имени В.Я. Кикотя, Москва, Россия

¹ kostin62@mail.ru

² vgonchar8@mvd.ru

Аннотация. Актуализируется проблема информационного деструктивного воздействия преступников на граждан в форме психологических операций и активных информационных мероприятий с помощью технических средств, специальных методов и приемов, способов и средств манипулирования общественным и индивидуальным сознанием. Отмечается распространенность в Российской Федерации телефонного мошенничества (вишинга), противодействие которому должно быть основано на комплексном подходе с помощью совокупности научных методов. Предлагается осуществление междисциплинарного анализа сведений о мошенниках: технологической оснащенности, манипулятивно-психологическом обеспечении, криминальном опыте и его изменчивости, индивидуально- и социально-психологических особенностях личности мошенников и их групп. Раскрываются результаты психологического анализа телефонных звонков мошенников, специализирующихся на хищениях с банковского счета и электронных денежных средств или конфиденциальной информации с помощью методов и приемов нейролингвистического программирования (НЛП), коммуникативных психологических приемов и речевых алгоритмов. Излагаются психологические рекомендации гражданам по вопросам цифровой самообороны от телефонных мошенников, основанные на результатах проведенного исследования.

Ключевые слова: информационное деструктивное воздействие, телефонное мошенничество, манипулятивное психологическое воздействие, противодействие преступлениям в сфере информационных технологий, социальная инженерия, хищение с банковского счета и электронных денежных средств

Для цитирования: Костина Л. Н., Гончар В. В. Необходимость применения комплексного подхода в противодействии телефонному мошенничеству // Вестник Московского университета МВД России. 2023. № 7. С. 289–295. <https://doi.org/10.24412/2073-0454-2023-7-289-295>. EDN: RBRDZO.

Original article

The need for a comprehensive approach to countering telephone fraud

Lyubov N. Kostina¹, Vladimir V. Gonchar²

^{1,2} Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot', Moscow, Russia

¹ kostin62@mail.ru

² vgonchar8@mvd.ru

Abstract. The problem of information destructive impact of criminals on citizens in the form of psychological operations and active information activities with the help of technical means, special methods and techniques, ways and means of manipulating public and individual consciousness is actualized. The prevalence of telephone fraud (vishing) in the Russian Federation is noted, the counteraction of which should be based on an integrated approach using a set of scientific methods. It is proposed to carry out an interdisciplinary analysis of information about scammers: technological equipment, manipulative psychological support, criminal experience and its variability, individual and socio-psychological characteristics of the personality of scammers and their groups. The results of the psychological analysis of phone calls of fraudsters specializing in theft from a bank account and electronic money or confidential information using methods and techniques of neuro-linguistic programming (NLP), communicative psychological techniques and speech algorithms are disclosed. Psychological recommendations to citizens on issues of digital self-defense against telephone scammers, based on the results of the study, are presented.

Keywords: information destructive impact, telephone fraud, manipulative psychological impact, countering crimes in the field of information technology, social engineering, theft from a bank account and electronic money

For citation: Kostina L. N., Gonchar V. V. The need for a comprehensive approach to countering telephone fraud. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2023;(7):289–295. (In Russ.). <https://doi.org/10.24412/2073-0454-2023-7-289-295>. EDN: RBRDZO.

© Костина Л. Н., Гончар В. В., 2023



Ни одна война никогда не начиналась и не велась без информационного воздействия, изменялись только технологии, в том числе психологические. Один из таких методов отмечает китайский философ Сунь Цзы в трактате «Искусство войны»: «Подрывайте престиж руководства противника, разжигайте ссоры и столкновения среди граждан, обесценивайте традиции, ...». Актуальность темы статьи определяется тем, что в современном мире информационное преступное воздействие на граждан реализуется в форме психологических операций и активных информационных мероприятий с помощью специальных методов и приемов, способов и средств манипулирования общественным и индивидуальным сознанием. Каждый человек в определенной степени внушаем, и это свойство усиливается в условиях неопределенности, напряженной обстановки и непредсказуемости. Психологический расчет преступников очевиден для достижения корыстных и иных целей: изменить сознание человека/граждан и подтолкнуть их к желаемым действиям и решениям.

В связи с быстрыми изменениями в системе социальных отношений ввиду интеграции во все сферы человеческой жизнедеятельности информационных технологий, резко возрастает необходимость эффективного использования специальных технических средств и психологических знаний в целях выявления инцидентов и профилактики деструктивного информационного воздействия на людей. Именно знание и понимание этих инцидентов, в основе которых лежит психологическое манипулирование, позволяет предупреждать мошенничество. Поэтому цитата «И если часто повторять удары, хоть мал топор, но дуб могучий срубит» (Уильям Шекспир. Король Генрих IV) имеет двойной смысл. Во-первых, неоднократно деструктивных действий мошенников (в лице отдельного лица или организованной преступной группы) усиливает эффект достижения криминальных целей. Об этом свидетельствует криминальная деятельность организованных на государственном уровне компаний со стороны зарубежных спецслужб по духовной деморализации граждан, воздействуя на сознание пользователей в сегментах сети Интернет. Усилим сказанное утверждением Оноре де Бальзака: «Там, где все горбаты, стройность становится уродством». Во-вторых, противоборство с мошенничеством должна обеспечиваться комплексом научно выверенных и грамотных методов, разработанных

специалистами (юристами, психологами, педагогами, сотрудниками правоохранительных органов и др.) и рассчитанных на возрастно-половые и индивидуально-психологические особенности различных категорий граждан. Подчеркнем, что в условиях «цифровой революции» именно достижения науки и техники, и в последствии осуществление комплексного подхода, интеграции автоматизированных и интеллектуальных систем, выступающих в качестве поддержки при принятии оперативно-тактических и (или) оперативно-служебных решений, становятся ключевым фактором трансформации и оптимизации деятельности правоохранительных органов.

В современных условиях распространены следующие типовые информационные преступные акции: размещение в сети информации — в форме текста, фото- или видеоматериалов о потерях личного состава и военной техники; распространение ложных сведений с помощью телефонной связи; угроза распространения персональных данных; популяризация преступной деятельности; создание фейкового контента с целью дискредитации тех или иных лиц и т. д. Признаки, по которым следует распознавать активность субъекта-мошенника, зависят от среды распространения. В случае получения текстовых сообщений в сети (социальные сети/мессенджеры) следует обращать внимание на следующие признаки, указывающие на мошенничество: 1) наличие вложений (закрепленные файлы); 2) обезличенную форму обращения; 3) отсутствие либо недостоверность контактных сведений; 4) домен, не относящийся к организации; 5) отчетливо прослеживающийся мотивационный формат к совершению вменяемых действий (при тщательном семантическом анализе текстовой информации) и др. в зависимости от среды передачи данных. Сочетание двух-трех признаков в поведении лица (отправителя той или иной информации) является основанием для того, чтобы насторожиться и не предпринимать активных действий, т. е. не стать жертвой мошенничества.

На сегодняшний день наиболее распространенным является телефонное мошенничество (так называемый вишинг) с применением сотовой связи, электронной почты, социальных сетей как аккумулирующих площадок людей/пользователей путем мотивирования держателя (платежной карты, аккаунта, социальной сети и пр.) к совершению определенных действий с целью получения финансовых средств,



конфиденциальной информации этого держателя. Очевидно, что противодействие телефонному мошенничеству должно быть основано на комплексном подходе, осуществление которого включает применение совокупности научных методов. В первую очередь, необходимо осуществление комплексного анализа действий мошенников. Речь идет о междисциплинарном анализе сведений о преступниках (как отдельных лиц, так и преступных групп — полноценно развернутых колл-центров, других соучастников преступления) и их действиях:

1) *технологическая оснащенность* (абонентский номер/номера, IMEI, IP/MAC-адреса, адрес электронной почты, социальная сеть), особенности их применения и изменений в зависимости от времени суток, года, адресата воздействия (категории и психологии граждан) и пр.;

2) *манипулятивно-психологическое обеспечение* (психологическое воздействие на жертву с помощью методов, приемов и средств общения; их алгоритмичность, гибкость и изменчивость);

3) *криминальный опыт* (алгоритмичность в мошеннических действиях, навыках и умениях — информационных, коммуникативных, психологических, тактических и др.) и его изменчивость в зависимости от объективных и субъективных факторов: непредвиденных обстоятельств, в ситуации дополнительного риска, поведения жертвы и т. д.;

4) *индивидуально-психологические особенности личности мошенника* (возрастно-половые и национальность; язык, речь, мышление и их гибкость; манера поведения и ее изменчивость/шаблонность; характер, способности и др.) и/или *социально-психологические особенности группы мошенников* (численный состав, наличие групповых норм, продолжительность совместной преступной деятельности, теснота взаимодействия в группе, уровень сплочения и пр.). Указанные категории лиц, связанные с определенным человеком или группой лиц, будут «перекликаться» с определенным «уровнем интенсивности взаимодействия» между собой, отражая определенный признак или их совокупность, устанавливающие «вес» сведений, степень вины и как результат установление личностей и идентификацию событий, к которым исследуемые объекты причастны.

Подчеркнем необходимость и научно-прикладной характер таких сведений, которые могут быть получены для решения научно-исследовательских,

профилактических, оперативно-розыскных, следственных целей только за счет привлечения к комплексной исследовательской работе специалистов из различных областей знаний.

В рамках первой группы сведений (технологическая оснащенность) необходимо обратить внимание на то, что с одного сотового аппарата (имеющего уникальный номер IMEI), могло использоваться несколько SIM-карт с абонентскими номерами. Установление лица (правонарушителя, т. е. инициатора коммуникации, который выполняет роль сотрудника банка, сотрудника правоохранительного органа, покупателя и пр.) определяется технической природой данного типа передачи данных (в классическом виде, который представляет собой: источник — среду — приемник). Более того, существуют компоненты, посредством анализа которых возможна процедура установления личности, — например анализ голоса говорящего, посредством которого возможно установить конкретного фигуранта.

Решение задач в рамках выделенных других групп сведений требует проведения тщательной, комплексной, оперативной и аналитической работы с аудиозаписями телефонных звонков. Осознавая актуальность и важность получения такой информации, авторами был проведен психологический анализ тридцати телефонных звонков мошенников. Раскрытым результатам этого исследования в виде указания конкретных манипулятивных психологических приемов, используемых этими лицами (Вишерами) в общении с гражданами (Клиентами). Сведения о том, как психологически Вишер/Вишеры обеспечивают работу и добиваются получения финансовых средств или конфиденциальной информации, представлены в табл. 1 в обобщенном виде. Отметим, что весь процесс общения основан на применении телефонными мошенниками методов и приемов нейролингвистического программирования (НЛП), коммуникативных психологических приемов и речевых алгоритмов [1, с. 42–46]. Процесс телефонного общения Вишеров с Клиентами был условно разделен на несколько этапов в соответствии с целями, которые достигались на каждом из этапов.

Психологический анализ телефонных разговоров мошенников показал, что схемы манипулирования отличаются в зависимости от уровня грамотности клиентов. Так, часть разговоров рассчитаны на более продвинутых Клиентов как пользователей банков-



Таблица 1

Используемые манипулятивные методы и приемы	Психологический расчет
1. Этап завоевания доверия за счет создания образа «авторитетного человека», атмосферы уважения личности Клиента и «защиты» от возникшей опасности	
Представление Вишера «авторитетным лицом» (сотрудником банка, полиции, др. организации)	Психологический прием, рассчитанный на завоевание у Клиента доверия
Сообщение неожиданной или неизвестной, опасной информации (оперативное информирование о том, что две минуты назад от имени Клиента была подана заявка)	Создание эффекта неожиданности (ОПАСНОСТЬ лишения денежных накоплений, конфиденциальных данных и пр.), оказывающий влияние на эмоциональную сферу психики и тем самым снижение рациональности и внимательности Клиента
Прямое или косвенное указание на ограниченность временных рамок действий, которые обеспечит Вишер как «авторитетное лицо»	Психологическое оперативное прямое воздействие: Мы бдительны, охраняем Вас; мы — СКОРАЯ ПОМОЩЬ, МЫ сейчас ЕЕ ОКАЗЫВАЕМ! Расчет на сочетание созданного эффекта неожиданности с ЧУВСТВОМ БЕЗОПАСНОСТИ
Неоднократное обращение по имени к Клиенту; подстройка к клиенту, ритму и темпу речи, копирование манеры разговора Клиента)	Психологический прием, рассчитанный на проявление уважения к личности Клиента, дополнительное ПОЗИТИВНОЕ ЭМОЦИОНАЛЬНОЕ ПОДКРЕПЛЕНИЕ с эффектом неожиданности и чувством безопасности
2. Этап подтверждения Клиентом его непричастности, квалификация действий как мошеннических и сообщение о том, что безопасность Клиента будет «обеспечена»	
Выяснение причастности клиента к подаче заявки: «Вы совершали действия?»	Заинтересовать Клиента в необходимости поддержания разговора и в том, чтобы получить положительный ответ — этого не делал Клиент (ПОЗИТИВНОЕ ЭМОЦИОНАЛЬНОЕ ПОДКРЕПЛЕНИЕ)
Переключение внимания Клиента, констатация факта и квалификация преступления: «Значит это мошенничество, мы будем разбираться и обеспечивать Вашу личную (!) безопасность»	Расчет на подкрепление чувства безопасности Клиента, вызов симпатии и доверия: МЫ АВТОРИТЕТНЫЕ ЛИЦА И ПРОФЕССИОНАЛЫ, у нас все под контролем, мы (ТОЛЬКО МЫ ПОМОЖЕМ ВАМ!); регуляция эмоционального состояния Клиента
Прямое или косвенное указание на ограниченность временных рамок действий	Расчет на то, чтобы Клиент в условиях ограниченности времени не смог разумно оценить реальность происходящего и самостоятельно предпринимать действия, акцент на том, что ОНИ КОНТРОЛИРУЮТ СИТУАЦИЮ
3. Этап управления вниманием Клиента, проверки эффективности воздействия на него и подготовка Клиента к выполнению нужных действий	
Последовательное информирование Клиента в спокойной манере и размеренном темпе о действиях, которые необходимо предпринять для того, чтобы оказать помощь Клиенту в сложившейся ситуации; предоставление информации с помощью официальных терминов, понятий, логических выводов и пр.	Психологический расчет на концентрирование внимания и интеллектуальные способности Клиента, ПОДГОТОВКА ЕГО К СОВЕРШЕНИЮ НУЖНОГО АЛГОРИТМА ДЕЙСТВИЙ. Расчет также состоит в том, что на слух информация воспринимается большинством людей не в полном объеме, что усиливает эффект воздействия
Использование обратной связи в виде последовательно задаваемых вопросов Клиенту	Убедиться в адекватности реагирования на вопросы, не критическом восприятии Клиентом информации и установке своеобразного диагноза: «КЛИЕНТ НАШ!»
«Да-техника» в виде вопросов, предполагающих получить утвердительный ответ «да»	Расчет на инертность психики и приведение Клиента в спокойное состояние, подготовка его к главному вопросу, связанному с непосредственным согласием на выполнение нужного алгоритма действий



Таблица 1 (окончание)

Используемые манипулятивные методы и приемы	Психологический расчет
4. Этап закрепления доверия и авторитета Вишера/-ов, которые «здесь и сейчас» будут «обеспечивать финансовую безопасность» Клиента реальными действиями	
Подчеркивание положительных качеств и заслуг Клиента: в банке он не был, не производил замену номера, не производил попытку перевода и пр.	Комплиментарный прием рассчитан на поддержание и сохранение лица Клиента и его самоуважения, чтобы вывести умозаключения — это вмешались злодеи, банки-конкуренты («недружественные» нам банки). Расчет на то, что ответа «Да» на ранее поставленный вопрос будет принят также (без критического осознания того, как это стало возможно и причем тут представители другого банка?)
Переключение клиента на необходимость выполнения действий, которые разъясняются официальным, юридическим языком, уже в более быстром темпе	Расширение воздействия на Клиента, объяснение НЕОБХОДИМЫХ ДЕЙСТВИЙ , обеспечивающих финансовую безопасность (тем самым продолжает закрепляться связь между АВТОРИТЕТОМ ВИШЕРА, ВНЕШНИМ КОНТРОЛЕМ СИТУАЦИИ, ОПЕРАТИВНЫМИ ДЕЙСТВИЯМИ, БЕЗОПАСНОСТЬЮ
5. Этап переключения на обычные финансовые действия Клиента и перестройка его на правила игры, которые нужны Вишерам	
Уточнение последних операций, остатков	Проверка доверия со стороны Клиента (если говорит обо всех счетах, остатках на них и пр.), то очевидно цель достигнута («НАШ КЛИЕНТ»), бдительность которого снижена, ОПАСНОСТИ НЕТ, СИТУАЦИЯ ПОД КОНТРОЛЕМ
Сбор исчерпывающей информации о вкладах, зарплате, пенсии, взаимодействии с другими банками и пр. для следующей Подчеркивание уважения к Клиенту, который готов превратиться в Жертву	Расчет на дальнейшее воздействие на Клиента, у которого «УСЫПИЛИ» БДИТЕЛЬНОСТЬ ; предупреждение в уважительной форме о том, что дальнейшая работа будет проводиться со специалистом; ОЦЕНКА ГОТОВНОСТИ К ПРОДОЛЖЕНИЮ КОНТАКТА ПО ТЕЛЕФОНУ СО СПЕЦИАЛИСТОМ

скими картами и программой Сбербанк-онлайн. Отличия коммуникативного диалога с такими Клиентами заключаются в следующем:

1) в употреблении слов-реагирований на ответы Клиента «зафиксировал», вопросов-подсказок «Возможно, Вы совершали...?»;

2) оформлении официальных документов — «протокола»;

3) подчеркивание преимуществ Сбербанка;

4) формулировкой вопроса: «имеется ли в настоящее время у Вас доступ к Интернету?»;

5) дополнительное использование различных манипулирования Клиента (по принципу: «Может, что-то сломается!») в виде конкретных команд, указаний («Включайте мобильное устройство»), пожеланий («Нужно обналить...»), указание негативных последствий («потеряете процентную ставку»), предложений по дополнительной помощи Клиенту (подключение сотрудников предварительного следствия и пр.).

Существуют также отличительные признаки в телефонных разговорах с Клиентами, с недостаточно высоким уровнем грамотности и осведомленности. Вишеры в таких ситуациях максимально удерживают время общения с Клиентом для достижения цели (превращения Клиента в Жертву) и перевод для общения по телефону с другим Специалистом. Следует также отметить некоторые отличия от проанализированной идеальной схемы:

1) меньшая грамотность с психологической точки зрения;

2) отсутствие поэтапности телефонного разговора (либо схема не отработана, либо это является проявлением индивидуального стиля мошенника);

3) однообразие фраз в виде реакций на ответы Клиента («понял», «понимаю...»);

4) неоднократное возвращение клиента к вопросу о длительности работы (что может вызвать подозрения у Клиента о том, что это звонит мошенник);



5) использование угроз как крайней меры (метода) психологического воздействия на Клиента — «самостоятельно разбирайтесь со своими проблемами», «будут заморожены счета» и пр.

Таким образом, действия телефонных мошенников заключается в изменении мотивации Клиента для выполнения им сиюминутной задачи «единственно верным алгоритмом действий» за счет эффекта неожиданности/новизны/неопределенности возникшей ситуации и вызванными негативными эмоциональными переживаниями. В таком состоянии Клиенту не понимает и не знает, что делать. Поэтому завоевание авторитета и доверия мошенники сочетают с внушением Клиенту идей о том, что безопасность может быть обеспечена с помощью определенных оперативных действий. Осуществляемый ими контроль и алгоритм действий выступает показателем того, что Клиент управляем, и он превращается в Жертву. Стоит также отметить, что для осуществления противодействия телефонному мошенничеству необходимы знания о жертвах этих преступлений. Такие знания в научной литературе указываются: люди возраста 50+, выраженными ценностями безопасности, образом мышления наивного оптимиста, высоким самоконтролем, ставящие интересы группы выше собственных, склонные к сотрудничеству [2]. Адресный характер профилактических мер в отношении этих лиц очевиден, как и очевидно и следующее: чтобы сломать отработанные мошеннические алгоритмы, которые способны запутать даже специалистов, при разговоре по телефону с незнакомцами или по незнакомому телефону, важно:

- ◆ помнить, что та должность, которой представился звонящий Вам человек — это всего лишь слова, ничем не подтвержденные. Определившийся номер телефона может быть подменным. Если вам поступил подозрительный звонок, прервите разговор, положив трубку, и перезвоните сами в организацию, от имени которой к Вам обратились;

- ◆ внимательно слушать, что Вам говорят, а также фоновые детали. Неуверенный голос, странные шумы за «кадром», путаница в названии организации и пр. указывают на то, что это звонят мошенники;

- ◆ осознавать и помнить, что обычно родственники звонят Вам лично. Поэтому, если звонят от имени Вашего родственника или знакомого и просят перевести деньги, положите трубку и перезвоните им лично. Даже если родственник/знакомый не подходит

к телефону — это не повод немедленно переводить деньги. Подождите, пока он перезвонит, или свяжитесь через других родственников/общих знакомых;

- ◆ подвергать критике и осознавать то, что Вам говорят. Необходимо задавать себе вопросы на понимание: «Почему он мне позвонил, так говорит?», «Откуда ему это известно?» и т. д.;

- ◆ осознавать и помнить, что конфиденциальные данные — о ваших банковских счетах и картах, пин-код или CVV/CVC/CVP-код, код из СМС — являются секретными (т. е. Вашими!!!) и не подлежат разглашению;

- ◆ осознавать и помнить, что правоохранительные органы, финансово-кредитные учреждения, другие организации не совершают юридически значимые действия по телефону, особенно в срочном порядке. Даже если вам угрожают уголовной ответственностью за отказ сотрудничать, сообщают, что за вами уже направлен наряд полиции — знайте, что телефонные угрозы не имеют юридической силы. При поступлении подобного звонка необходимо прервать разговор и перезвонить в соответствующее подразделение или организацию, чтобы узнать необходимую информацию;

- ◆ завершить телефонный разговор, если Вас настойчиво просят, требуют совершить определенные действия в режиме «здесь и сейчас», угрожают последствиями, если их не выполните;

- ◆ отрегулировать свое эмоциональное состояние, если переживаете после прекращенного Вами звонка: сделайте паузу, несколько глубоких вдохов-выдохов, позвоните близким людям и обсудите тревожную ситуацию, совместно и объективно оцените происходящее. Похвалите себя за то, что смогли противостоять мошеннику.

Подводя итоги, отметим, что комплексный подход в исследовании телефонного мошенничества вынужденная, необходимая и действенная мера, направленная на противодействие с этим распространенным видом преступности в Российской Федерации. Знание и постоянное научно-прикладное изучение сведений об алгоритмах, схемах, типичных признаках, информационно-техническом оснащении, психологических манипулятивных приемах телефонных мошенников, криминальном опыте и о психологических особенностях этих лиц направлено на эффективное обеспечение деятельности сотрудников правоохранительных органов, разъяснительную, право-



воспитательную и профилактическую работу с гражданами. Представленные психологические рекомендации граждан основаны на проведенном исследовании манипулятивных методов и приемов телефонных мошенников. В настоящее время возрастает роль индивидуальной правовой и психологической зрелости граждан [3, с. 58], призванной также противостоять мошенникам. Ловкой манипуляции сознанием, желанию нажиться на наших сбережениях, требованиям совершить «здесь и сейчас» определенные действия необходимо противопоставить неразглашение наших секретов (ПИН-кодов, паролей, CVV/CVC/CVP-кодов, кодов из СМС-сообщений), осознание того, что каждый из нас разумный и думающий человек, могущий прервать опасный звонок, объективно оценивающий происходящее и могущий самостоятельно получить необходимую или дополнительную информацию, помощь у своих родственников и близких людей, сотрудников правоохранительных органов, финансово-кредитных учреждений и иных организаций [4, с. 358].

Список источников

1. Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита. М. : ЧеРо, 1997.

2. Мешкова Н. В., Кудрявцев В. Т., Ениколопов С. Н. К психологическому портрету жертв телефонного мошенничества // Вестник Московского университета. Серия 14. Психология. 2022. № 1. С. 138–157.

3. Энциклопедия юридической психологии / под общ. ред. проф. А. М. Столяренко. М. : ЮНИТИ-ДАНА ; Закон и право, 2003.

4. Противодействие преступлениям, совершаемым в сфере информационных технологий: учебник / под науч. ред. И. А. Калиниченко. М. : Инфра-М, 2023.

References

1. Dotsenko E. L. Psychology of manipulation: phenomena, mechanisms and protection. M. : Chero, 1997.

2. Meshkova N. V., Kudryavtsev V. T., Enikolopov S. N. On the psychological portrait of victims of telephone fraud // Bulletin of the Moscow University. Episode 14. Psychology. 2022. № 1. P. 138–157.

3. Encyclopedia of Legal Psychology / ed. by Prof. A. M. Stolyarenko. M. : UNITY-DANA ; Law and Legislation, 2003.

4. Countering crimes committed in the field of information technology: textbook / ed. by I. A. Kalinichenko. M. : Infra-M, 2023.

Информация об авторах

Л. Н. Костина — начальник кафедры психологии учебно-научного комплекса психологии служебной деятельности Московского университета МВД России имени В.Я. Кикотя, доктор психологических наук, профессор;

В. В. Гончар — начальник кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент.

Information about the authors

L. N. Kostina — Head of the Department of Psychology of the Educational and Scientific Complex of the Psychology of Performance of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Doctor of Psychological Sciences, Professor;

V. V. Gonchar — Head of the Department of Information Security of the Information Technology Training and Research Complex of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Candidate of Legal Sciences, Associate Professor.

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.

Статья поступила в редакцию 30.11.2023; одобрена после рецензирования 08.12.2023; принята к публикации 18.12.2023.

The article was submitted 30.11.2023; approved after reviewing 08.12.2023; accepted for publication 18.12.2023.