ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI:10.21822/2073-6185-2023-50-2-109-116 Обзорная статья / Review Paper

Претекстинг и способы противодействия ему

У.А. Михалёва
Северо-восточный федеральный университет им. М.К. Аммосова,
677000, г. Якутск, ул. Белинского, д. 58, Россия

Резюме. Цель. В настоящее время мошенничество является одной из наиболее актуальных проблем в современном обществе. Количество жертв мошенников, использующих методы социальной инженерии изо дня в день растет. Мошенничество – это вид преступления, которое очень сложно доказать. Целью исследования является поиск способа противодействия претекстингу как повышение информационной безопасности населения. **Метод.** В данной статье используются следующие методы: описание, анализ, дедукция. **Результат**. Проведенный анализ описания методов социальной инженерии позволил классифицировать их по способу воздействия на человека. Также данный анализ позволил сделать вывод, что самым эффективным способом защиты от угроз социальной инженерии, в частности, от претекстинга является внедрение технических способов защиты. **Выводы.** Выводы, сделанные в данной работе, могут послужить основанием для дальнейших исследований по направлению, а также основанием для разработки и внедрения технических способов защиты от угроз претекстинга.

Ключевые слова: мошенничество, социальная инженерия, претекстинг, фишинг, смишинг, кви про кво, дорожное яблоко, троян, обратная социальная инженерия, плечевой серфинг

Для цитирования: У.А. Михалёва. Претекстинг и способы противодействия ему. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(2):109-116. DOI:10.21822/2073-6185-2023-50-2-109-116

Pretexting and means to counter it

U.A. Mikhaleva
M.K. Ammosov North-Eastern Federal University,
58 Belinsky St., Yakutsk 677000, Russia

Abstract. Objective. Currently, fraud is one of the most pressing problems in modern society. The number of victims of scammers using social engineering methods is growing day by day. Because fraud is a type of crime that is very difficult to prove. The aim of the study is to find a method to counteract pretexting as an increase in the information security of the population. **Method.** This article uses the following methods: description, analysis, deduction. **Result.** The analysis of the description of social engineering methods made it possible to classify them according to the way they influence a person. Also, this analysis led to the conclusion that the most effective method to protect against the threats of social engineering, in particular, from pretexting, is the introduction of technical methods of protection. **Conclusion.** The conclusions made in this work can serve as a basis for further research in this direction, as well as the basis for the development and implementation of technical methods for protecting against pretexting threats.

Keywords: fraud, social engineering, pretexting, phishing, mixing, qui about quo, road apple, Trojan, reverse social engineering, shoulder surfing

For citation: U.A. Mikhaleva. Pretexting and means to counter it. Herald of Daghestan State Technical University. Technical Science. 2023; 50(2):109-116. DOI:10.21822/2073-6185-2023-50-2-109-116

Введение. По информации отчета Федеральной службы по финансовому мониторингу «О проведении национальной оценки рисков отмывания денег и финансирования терроризма» в качестве ключевых угроз отмывания преступных доходов отмечена мошенническая деятельность первой из всех возможных преступных деятельностей [1]. Мошенничество, согласно ст. 159 УК РФ – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием [2].

В настоящее время мошенничество с использованием методов социальной инженерии является одним из самых распространенных атак.

По результатам отчета «Актуальные киберугрозы: итоги 2022 года» Российской компании Positive Technologies социальная инженерия по-прежнему оказалась на высоте. По их данным, в успешных атаках на организации этот метод применялся в 43% случаев, на частных лиц — в 93% [3].

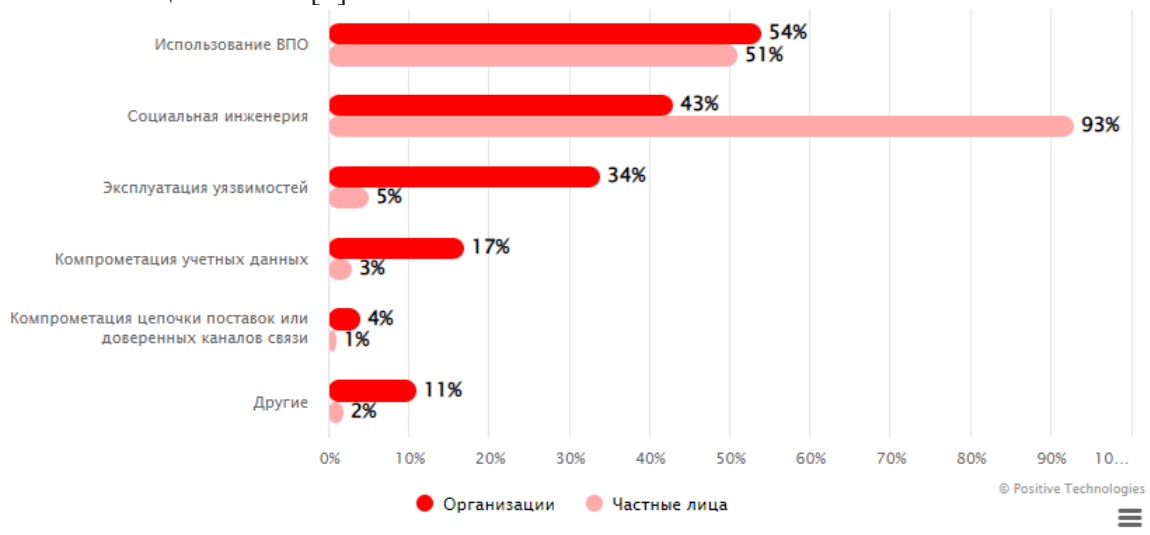

Рис. 1. Методы атак (доля успешных атак) [3]
Fig. 1. Attack methods (percentage of successful attacks) [3]

По информации Центробанка Российской Федерации в 2022 году больше половины случаев кражи средств граждан было совершено именно с помощью социальной инженерии. Размер ущерба от действий злоумышленников вырос на 4,29%, до 14,2 млрд. рублей [4]. Вышеприведенные отчеты показывают, что угрозы атак социальной инженерии возрастают. Это связано с тем, что как бы не совершенствовались технические системы защиты, самым слабым звеном все еще остается человек. Его слабости, стереотипы, предрассудки и т.п. являются наибольшей угрозой системе информационной безопасности.

Постановка задачи. Так как социальная инженерия активно ориентируется на особенности человеческой натуры, жертвой может стать кто угодно. Осознание данного факта приводит к необходимости защиты конфиденциальных данных вне зависимости от психологического и эмоционального состояния человека. Для обеспечения должного уровня защиты конфиденциальной информации населения необходимо создать универсальный способ защиты от угроз социальной инженерии. В рамках данного исследования рассмотрим способы защиты конфиденциальной информации от претекстинга.

Методы исследования. Социальная инженерия представляет метод получения необходимого доступа к конфиденциальной информации, используя социальные и психологические воздействия на людей [5-10].

Атака на людей с использованием методов социальной инженерии бывает разной. Ниже приведем основные методы социальной инженерии:

1. Подложные предложения и ссылки. Жертве поступают предложения о выигрыше в лотерее, подарке от известного бренда, замаскированные ссылки на известные сайты с выгодными предложениями, уведомления о необходимости установить ПО для

защиты компьютера. После перехода по ссылкам происходит кража данных, которые жертва вводит в предложенной форме или устанавливается вредоносное ПО, похищающее информацию [11].

2. Фишинг. Метод сбора пользовательских данных для авторизации — обычно это массовые рассылки спама по электронной почте. В классическом сценарии на почту жертвы приходит поддельное письмо от какой-то известной организации с просьбой перейти по ссылке и авторизоваться. Чтобы вызвать больше доверия, мошенники придумывают серьёзные причины для перехода по ссылке: например, просят жертву обновить пароль или ввести какую-то информацию (ФИО, номер телефона, банковской карты и даже CVV-код) [12].
3. Телефонный фишинг и фрикинг. Реализуется путем отправки пользователю голосовых сообщений от несуществующих банков с целью получения пин-кодов карты или одноразовых паролей для проведения финансовых операций. Также здесь может использоваться перехват сигналов тонового набора служебных сигналов во время телефонных звонков [11].
4. Смишинг – это разновидность фишинга, попытка получить данные посредством SMS-сообщений [13-14].
5. Претекстинг. Мошенник представляется подложной персоной и действует по заранее подготовленному сценарию, располагает частью знаний о человеке. Это может быть псевдосотрудник государственных организаций или внутренних органов, который выманивает у жертвы конфиденциальные данные [11].
6. Кви про кво (услуга за услугу). Атака построена на обращении злоумышленника в интересующую компанию под видом ее персонала по вопросу предоставления ему услуги техподдержки на рабочем месте. Это помогает украсть данные учетных записей и запустить нежелательные процессы [11].
7. Дорожное яблоко (ловля «на живца»). Реализуется путем подброса физических носителей информации на территорию интересующей компании, на которых присутствует вредоносный код. Это могут быть CD-диск, флеш-накопитель. Они специально маркируются логотипами и цветами компании, содержат приглашение для использования вроде надписей: «Строго секретно», «Коммерческая тайна», «Доходы компании». Сотрудник использует носитель на своем рабочем месте, после чего происходит кража данных [11].
8. Плечевой серфинг. Основывается на невнимательности жертвы, которая уверена в своей безопасности и никак не защищает конфиденциальные данные. Злоумышленник осуществляет контакт в общественном месте с жертвой и свободно подсматривает информацию, которая находится в открытом доступе на экранах мобильных устройств [11].
9. Обратная социальная инженерия. Основывается на доверии к незнакомому человеку, когда жертва добровольно сообщает конфиденциальные данные злоумышленнику. Это характерно при обращении в техподдержку по вопросам блокировки или прекращения доступа. Жертва, желая помочь и ускорить процесс разблокировки сама, сообщает пин-коды, одноразовые пароли, идентификаторы в системе, не подозревая о том, что это может быть использовано против нее. Встречается чаще всего внутри крупных компаний, где коллеги обманывают друг друга или имеют доступ к информации, которая изначально для них закрыта [11].
10. «Ты – мне, я – тебе». Говорят, честный обмен – не грабеж, но не в этом случае. Многие социальные инженеры убеждают своих жертв в том, что те получат что-то в обмен на данные или доступ к ним. Так работает фальшивый антивирус, предлагающий пользователю устранить угрозу на его компьютере, хотя сам «антивирус» и есть угроза [13-14].

11. Взлом электронной почты и рассылка по контактам. Злоумышленник взламывает почту человека или его учетную запись в социальной сети, получая доступ к его контактам. От имени жертвы он может сообщить им, что его ограбили, и попросить перечислить ему денег, или разослать ссылку на вредоносное ПО, или клавиатурный шпион под видом интересного видео [13-14].
12. Троян. Вирус не зря получил своё название по принципу работы троянского коня из древнегреческого мифа. Только приманкой здесь становится email-сообщение, которое обещает быструю прибыль, выигрыш или другие «золотые горы» — но в результате человек получает вирус, с помощью которого злоумышленники крадут его данные. Почему этот вид кражи данных называют социальной инженерией? Потому что создатели вируса хорошо знают, как замаскировать вредоносную программу, чтобы вы наверняка кликнули по нужной ссылке, скачали и запустили файл [13-14].

Перечисленные выше методы социальной инженерии на практике могут быть использованы в комбинации друг с другом в зависимости от ситуации.

Описание приведенных методов социальной инженерии приводит к классификации угроз, которые влияют на личные качества жертвы. В табл. 1 приведена классификация методов социальной инженерии, которые влияют на личные качества жертвы. Их можно классифицировать по следующим типам: наивность, жадность, доверчивость, любопытство.

Таблица 1. Классификация методов социальной инженерии, которые влияют на личные качества жертвы

Table 1. Classification of social engineering methods that affect the personal qualities of the victim

№	Наивность/Naivete	Жадность/ Greed	Доверчивость/Credulity	Любопытство/ Curiosity
1	Фишинг/ Phishing	Троян/ Trojan	Подложные предложения и ссылки/ Fake offers and links	Кви про кво/Qui pro quo
2	Плечевой серфинг/ Shoulder surf		Телефонный фишинг и фрикинг/ Phone phishing and phreaking	Дорожное яблоко (ловля «на живца»)/ Road apple (live bait fishing)
3	Ты – мне, я – тебе/ You to me, I to you		Смишинг/ Cmishing	
4	Взлом электронной почты и рассылка по контактам/Hacking email and sending to contacts		Обратная социальная инженерия/Reverse social engineering	
5	Претекстинг/ Pretexting			

Как видно из табл. 1, претекстинг может влиять на различные личные качества человека. Потому что, главное отличие претекстинга от других видов социальной инженерии – это внезапность и создание чувства страха, спешки в реальном времени. Решение должно быть принято незамедлительно, нет времени на переваривание информации.

Таким образом, на принятие решения влияют чувства, а не разум. Поэтому данный вид угрозы может играть на различные качества человека, такие как: желание помочь, сохранить имеющиеся средства, побыстрее решить возникшую проблему, также желание успеть заполучить быструю прибыль, быть среди «первых» для получения какого-то преимущества, не упускать шанс большого выигрыша и т.д.

Обсуждение результатов. Претекстинг подразумевает осуществление личного эмоционального контакта злоумышленника с жертвой. При этом злоумышленник имеет заранее продуманный сценарий действий. Он заранее знает личные сведения о жертве: окружение, семью, предпочтения, место работы и многое другое. Чаще всего всю эту информацию он

берет из социальных сетей. Изучив эти сведения, злоумышленник может представиться коллегой, знакомым коллеги, сотрудником правоохранительных органов, медицинского учреждения или банковских учреждений и т.д. Он осуществляет атаку по телефону. При этом, номер абонента может быть подменен на номера знакомого, организации, учреждения. С технической точки зрения, подмена номера телефона или голоса делается с помощью программных продуктов [15-16].

В настоящее время основными способами защиты от атак вида претекстинг, являются:

1. Информирование населения о возможных действиях мошенников через средства массовой информации;
2. Составление черного списка телефонных номеров и их автоматическая блокировка в приложениях кредитно-финансовых организаций на основе отчетов правоохранительных органов;
3. Использование антифрод-платформы в телекоммуникационных сетях связи.

По информации телеком-организаций, антифрод-решение отличает звонки из клиентской службы банка от звонков мошенников даже при использовании подменных номеров и помогает препятствовать незаконному выводу денег со счетов клиентов [17].

Существующие технические методы противостояния атакам претекстинга основаны на анализе произошедших атак, зафиксированных в правоохранительных органах. Это, конечно, немного сокращает глобальный рост жертв, но в то же время полностью не решает существующую проблему телефонного мошенничества.

Вопросами решения данной проблемы занимаются не только правоохранительные органы, кредитно-финансовые и телеком-организации. Данная тема также привлекает и научные организации.

В работах авторов научных статей [18-20] описаны методы противодействия претекстингу, но они носят в основном информативно-рекомендательный характер.

В своей работе [21] автор цитирует работу автора статьи «Социальная инженерия и кибербезопасноть: виктимологический аспект»: «универсального средства защиты от техник социальной инженерии не существует. Даже надежно защищенная при помощи новейших технических и аппаратных средств и изолированная от сети Интернет информационная система уязвима к атакам подобного рода, потому что с ней работают и ею управляют люди. Весь вопрос лишь в том, насколько изощренную и достоверную схему обмана сможет придумать социальный инженер, чтобы войти в доверие и принудить жертву совершить требуемые и заранее спрогнозированные действия» [22].

Похожий вариант решения в борьбе с угрозами социальной инженерии предложили авторы статьи [23]. Они предложили создание программного комплекса, базирующегося на алгоритмах обработки естественного языка в режиме реального времени, используя метод BERT. Авторы отмечают, что «приложение, базирующееся на данном программном комплексе, будет иметь ряд преимуществ относительно уже существующих продуктов:

1. Обработка непосредственно смысловой нагрузки разговора, позволяющая обнаруживать атаки независимо от того, производились звонки с этого номера телефона ранее или нет;
2. Результат анализа в режиме реального времени, то есть приложение позволяет моментально пресекать возможную атаку со стороны мошенников, не дожидаясь того, когда данный номер телефона будет помечен одним из пользователей;
3. Объективная оценка, не зависящая от личностных качеств и предубеждений пользователей приложения;
4. Безопасность приложения, обусловленная тем, что для функционирования данного программного комплекса не требуется предоставлять доступ к персональной информации, например, к номерам контактных телефонов, записанных на устройстве» [23].

Похожий подход выдвинули авторы статьи [24]. Они предлагают использовать искусственный интеллект в распознавании мошенника по эмоции речи на основе анализа частот-

ных отклонений по каждой букве в диалоге. Предложенный метод выявляет факт эмоционального давления на собеседника.

Как видно, из проведенного исследования, в данное время нет единого универсального подхода или порядка действий для быстрого выявления мошенника в ходе разговора. Также не существует и решения, позволяющего автоматически обнаружить и блокировать звонок мошенника. Проведенное исследование говорит о необходимости разработки алгоритма автоматического обнаружения звонков мошенников. Одним из универсальных способов обнаружения звонков мошенников может явиться использование нейронной языковой модели, использующей семантический анализ речи.

Вывод. Особенностью использования методов социальной инженерии заключается в том, что сложно противостоять, сложно доказать и в настоящее время найти злоумышленника все еще остается трудоемким и трудозатратным процессом. Сколько бы ни информировали население о возможных действиях мошенников через средства массовой информации, все еще жертв от действий злоумышленников, применяющих методы социальной инженерии растет из года в год. Это связано с тем, что мошенники используют особенности человеческой натуры, такие как любопытство, жадность, доверие, уважение, желание помочь другу и т.д. Внедрение технического способа защиты на основе семантического анализа речи посредством нейронной языковой модели позволит предотвратить различные психологические манипуляции злоумышленника.

Библиографический список:

1. О размещении отчетов о проведении национальной оценки рисков отмывания денег и финансирования терроризма / Новости // Росфинмониторинг. – 23.12.2022. – URL: https://www.fedsfm.ru/releases/6236 (дата обращения 06.04.2023).
2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 03.04.2023) // Электронно-правовая база «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdf64b7c9cfd62e90d7f55f9b5b7b72b755/ (дата обращения 06.04.2023).
3. Актуальные киберугрозы: итоги 2022 года. / Аналитика // Российская компания, специализирующаяся на разработке решений в сфере информационной безопасности Positive Technologies. – 29.03.2023. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения 06.04.2023).
4. «Противодействие мошенничеству и социальной инженерии» с участием Председателя Банка России Эльвиры Набиуллиной / Новости // Банк России. – 16.02.2023. – URL: https://www.cbr.ru/press/event/?id=14556 (дата обращения 06.04.2023).
5. Митник, К.Д. Искусство обмана / К.Д. Митник, В.Л. Саймон // Компания АйТи. – 2004. – 360 с.
6. Ревенков, П.В. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания / П.В. Ревенков, А.А. Бердюгин // Национальные интересы: приоритеты и безопасность. – 2017. – № 9(354). – С. 1747-1760.
7. Старостенко, Н.И. Криминалистический аспект техник социальной инженерии при совершении преступлений / Н.И. Старостенко // Вестник Краснодарского университета МВД России. – 2020. – №1(47). – С 80-83.
8. Стеценко Ю.А., Холодковская Н.С. Мошенничество в сети Интернет / Ю.А. Стеценко, Н.С. Холодковская // Вестник Таганрогского института имени А.П. Чехова. – 2021. – №4. – С. 75-80.
9. Созаев, С.С. Социальная инженерия, ее техники и методы ее противодействия / С.С. Созаев, Д.А. Кунашев // Вестник науки: международный журнал. – 2020. – № 2(23). – Т. 1. – С. 85-88.
10. Годунова М.С., Копосова М.С. Социальная инженерия как метод киберпреступления / М.С. Годунова, М.С. Копосова // Научно-образовательный журнал для студентов и преподавателей «StudNet». –2022. – №6 – С. 5573-5580.
11. Социальная инженерия / Блог // ПАО «Ростелеком». – 17.02.2023. – URL: https://rt-solar.ru/events/blog/3331/ (дата обращения 06.04.2023).
12. Марзоев А.А., Софронов В.А., Щербаков Р.С. Социальная инженерия / А.А. Марзоев, В.А. Софронов, Р.С. Щербаков // Повышение обороноспособности государства 2022: сборник научных трудов по материалам заочной научной конференции. Изд. Санкт-Петербург: ООО «Полторак», 2022. С. 25-31.
13. Риски в сфере кибербезопасности и социальной инженерии / Последние новости России и Мира сегодня // Anticwar.ru. – 2022-06-10. – URL: https://anticwar.ru/riski_v_sfere_kiberbezopasnosti_i_sotsialnoiu_indjenerii_9714 (дата обращения 06.04.2023).

14. Как избежать атаки с использованием социальной инженерии / Угрозы // Официальный сайт АО «Лаборатория Касперского». – 06.04.2023. – URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (дата обращения 06.04.2023).
15. Зотина Е.В. Претекстинг как прием социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему / Е.В. Зотина // Вестник Казанского юридического института МВД России. – 2022. – №4(50). – С.93-99.
16. Котляр Е. О., Мещеряков М. О., Бугаев К. Г. Методы социальной инженерии как инструмент хищения конфиденциальных данных пользователей / Е. О. Котляр, М. О. Мещеряков, К. Г. Бугаев // Охрана, безопасность, связь. – 2021. – №6-2. – С. 223-230.
17. Телефонное мошенничество: как противодействовать обману / Аналитические статьи // Информационно-правовой портал Гарант.ру. –1.03.2021. – URL: https://www.garant.ru/article/1448451/ (дата обращения 06.04.2023).
18. Ламинина О.Г. Возможности социальной инженерии в информационных технологиях / О.Г. Ламинина // Гуманитарные, социально-экономические и общественные науки. – 2017. – №2. – С.21-23.
19. Репенко В.А., Резниченко С.А. Защита от атак с применением средств и методов социальной инженерии / В.А. Репенко, С.А. Резниченко // Вестник Дагестанского государственного технического университета. Технические науки. – 2022. – Том.49, № 4. – С.85-96.
20. Тепляков С.П., Тимохович А.С. Социальная инженерия. Анализ и методы защиты / С.П. Тепляков, А.С. Тимохович // ACADEMY. – 2018. – 7(34). – С.26-27.
21. Моторина В.О. Методы социальной инженерии в обесепечении информационной безопасности в организации / В.О. Моторина // Безопасность информационного пространства-2017: сборник научных трудов по материалам XVI всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Изд. Екатеринбург: «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», 2018. С. 281-284.
22. Унукович А. С. Социальная инженерия и кибербезопасноть: виктимологический аспект / А.С. Унукович // Психопедагогика в правоохранительных органах. – 2021. – Том 26, № 3(86). – С.346-351.
23. Частикова В.А., Гуляй В.Г. Методика обнаружения атак социальной инженерии на основе алгоритмов анализа естественного языка / В.А. Частикова, В.Г. Гуляй // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 3(59). – С.61-71.
24. Филимонов А.В., Осипов А.В., Плешакова Е.С., Гатауллин С.Т. Нейросетевые методы распознавания эмоций речи для противодействия мошенничеству в телекомукационных системах / А.В. Филимонов, А.В. Осипов, Е.С. Плешакова, С.Т. Гатауллин // Вопросы кибербезопасности. – 2022. – № 6(52). – С.83-92.

References:

1. On the placement of reports on the national assessment of the risks of money laundering and terrorist financing / News // Rosfinmonitoring. – 23.12.2022. – URL: https://www.fedsfm.ru/releases/6236 (accessed 06.04.2023). (In Russ)
2. Criminal Code of the Russian Federation form 13.06.1996 N 63-FL (ed. dated 03.04.2023) // Electronic legal base « Consultant Plus». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdf64b7c9cfd62e90d7f55f9b5b7b72b755/ (accessed 06.04.2023). (In Russ)
3. Actual cyber threats: results of 2022. / Analytics // Russian company specializing in the development of solutions in the field of information security Positive Technologies. – 29.03.2023. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (accessed 06.04.2023). (In Russ)
4. «Countering fraud and social engineering» with the participation of Elvira Nabiullina, Governor of the Bank of Russia / News // Bank of Russia. – 16.02.2023. – URL: https://www.cbr.ru/press/event/?id=14556 (accessed 06.04.2023). (In Russ)
5. Mitnik, K.D. The Art of Deception / K.D. Mitnik, V.L. Saimon. IT Co. 2004; 360. (In Russ)
6. Rebenkov, P.V. Social engineering as a source of risks in remote banking / P.V. Rebenkov, A.A. Berdyugin. *National Interests: Priorities and Security*. 2017; 9(354): 1747-1760. (In Russ)
7. Starostenko, N.I. Forensic aspect of social engineering techniques in the commission of crimes. *Herald of the Krasnodar University of the Ministry of Internal Affairs of Russia*. 2020;1(47): 80-83. (In Russ)
8. Stetsenko Y.A., Kholodkovskaya N.S. Fraud on the Internet / Y.A. Stetsenko, N.S. Kholodkovskaya. *Herald of the Taganrog Institute named after A.P. Chekhov*. 2021;4: 75-80. (In Russ)
9. Sozaev, S.S. Social engineering, its techniques and methods of countering it / S.S. Sozaev, D.A. Kunashev. *Science Herald: International Journal*. 2020; 2(23) (l. 1.): 85-88. (In Russ)
10. Godunova M.S., Koposova M.S. Social engineering as a method of cybercrime. *Scientific and educational magazine for students and teachers «StudNet»*. 2022;6:5573-5580. (In Russ)
11. Social engineering / Blog // PJSC « Rostelecom». – 17.02.2023. – URL: https://rt-solar.ru/events/blog/3331/ (accessed 06.04.2023). (In Russ)
12. Marzoev A.A., Sofronov V.A., Shcherbakov R.S. Social engineering / A.A. Marzoev, V.A. Sofronov, R.S. Shcherbakov. *Increasing the defense capability of the state 2022: a collection of scientific papers based on*

the materials of the correspondence scientific conference. Ed. St. Petersburg: Poltorak LLC. 2022; 25-31. (In Russ)

13. Риски в сфере кибербезопасности и социальной инженерии / Последние новости России и Мира сегодня // Anticwar.ru. – 2022-06-10. – URL: https://anticwar.ru/riski_v_sfere_kiberbezopasnosti_i_sotsialnoiu_indjenerii_9714 (accessed 06.04.2023). (In Russ)
14. How to avoid a social engineering attack / Threats // Official website of JSC "Kaspersky Lab". – 06.04.2023. – URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (accessed 06.04.2023). (In Russ)
15. Zotina E.V. Pretexting as a social engineering technique used by telephone scammers: a criminological view of the problem. *Herald of the Kazan Law Institute of the Ministry of Internal Affairs of Russia.* 2022;4(50):.93-99. (In Russ)
16. Kotlyar E. O., Meshcheryakov M. O., Bugaev K. G. Social engineering methods as a tool for stealing user confidential data. *Security, safety, communication*. 2021;6-2: 223-230. (In Russ)
17. Phone Fraud: How to Counteract Fraud / Analytical articles/ Information and legal portal Гарант.ру. –1.03.2021. – URL: https://www.garant.ru/article/1448451/ (accessed 06.04.2023). (In Russ)
18. Laminina O.G. Possibilities of social engineering in information technologies. *Humanities, socio-economic and social sciences.* 2017;2:.21-23. (In Russ)
19. Repenko V.A., Reznichenko S.A. Protection against attacks using social engineering tools and methods. *Herald of the Daghestan State Technical University. Technical Science.* 2022;.49(4):.85-96. (In Russ)
20. Teplyakov S.P., Timokhovich A.S. Social engineering. Analysis and protection methods. *ACADEMY*. 2018; 7(34):26-27. (In Russ)
21. Motorina V.O. Methods of social engineering in ensuring information security in an organization. Security of the information space-2017: collection of scientific papers based on the materials of the XVI All-Russian scientific and practical conference of students, graduate students and young scientists. Ed. Ekaterinburg: «Ural Federal University named after the first President of Russia B.N. Yeltsin», 2018; 281-284. (In Russ)
22. Unukovich A.S. Social Engineering and Cybersecurity: The Victimological Aspect. *Psychopedagogy in law enforcement.* 2021; 3(86):346-351. (In Russ)
23. Chastikova V.A., Gulyai V.G. Technique for detecting social engineering attacks based on natural language analysis algorithms. *Caspian Journal: Management and High Technologies*. 2022; 3(59):61-71. (In Russ)
24. Filimonov A.V., Osipov A.V., Pleshakova E.S., Gataullin S.T. Neural Network Methods for Recognizing Speech Emotions to Counter Fraud in Telecommunication Systems. *Cyber security issues.* 2022;6(52):.83-92. (In Russ)

Сведения об авторах:

Ульяна Анатольевна Михалёва, кандидат технических наук, доцент кафедры многоканальных телекоммуникационных систем института математики и информатики; uamikhaleva@mail.ru

Information about the authors:

Ulyana A. Mikhaleva, Cand. Sci. (Eng), Assoc. Prof., Department of Multichannel Telecommunication Systems of the Institute of Mathematics and Informatics; uamikhaleva@mail.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 23.04.2023.

Одобрена после рецензирования / Reviced 14.05.2023.

Принята в печать /Accepted for publication 14.05.2023.