УДК 343

Социальная инженерия в цифровую эпоху: анализ личности преступника и классификация программных инструментов

Владимир Валентинович Глазовский[1,2]
[1]Санкт-Петербургская академия Следственного комитета, Санкт-Петербург, Россия, vladimir.glazovsky@yandex.ru
[2]Следственное управление Следственного комитета Российской Федерации по Калужской области, Калуга, Россия

Аннотация. Представлен комплексный анализ преступлений, совершаемых с применением методов социальной инженерии, а также программного обеспечения, используемого злоумышленниками для достижения своей преступной цели. Согласно обнародованным Генеральной прокуратурой Российской Федерации данным в 2024 г. количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в том числе с применением методов социальной инженерии, увеличилось на 13 %. Автором проведен криминологический анализ личности преступников, совершающих преступления рассматриваемой категории, позволивший выделить их ключевые характеристики, среди которых: обладание навыками манипуляции с использованием трехэтапной эмоциональной модели, а также предварительная техническая подготовка преступников. Автором разработана классификация программного обеспечения, применяемого злоумышленниками при совершении преступлений с использованием методов социальной инженерии на основе их функционального назначения и цели применения. Особое внимание уделено механизмам противодействия преступлениям указанного вида. Результаты проведенного исследования позволяют разработать практические рекомендации для правоохранительных органов, направленные на идентификацию личности преступника посредством проведения анализа геолокационных данных и VPN-трафика злоумышленника.

Ключевые слова: социальная инженерия, личность преступника, киберпреступность, кибербезопасность, информационно-телекоммуникационные технологии, программное обеспечение, криминалистика, оперативно-розыскная деятельность

Для цитирования: Глазовский В.В. Социальная инженерия в цифровую эпоху: анализ личности преступника и классификация программных инструментов // Правда и закон. 2025. № 3(33). С. 106–114.

Social engineering in the digital age: criminal personality analysis and software tool classification

Vladimir V. Glazovsky[1,2]
[1]SK RF SPb Academy, St. Petersburg, Russia, vladimir.glazovsky@yandex.ru
[2]Investigative Department of the Investigative Committee of the Russian Federation for the Kaluga Region, Kaluga, Russia

Abstract. Presents a comprehensive analysis of crimes committed using social engineering techniques, as well as the software tools employed by offenders to achieve their illicit objectives. According to data published by the Prosecutor General's Office of the Russian Federation, in 2024 the number of crimes involving information and telecommunication technologies, including those utilizing social engineering methods, increased by 13 %. The author conducts a criminological analysis of the personality traits of offenders who commit such crimes, identifying key characteristics such as proficiency in manipulation using a three-stage emotional model, as well as advanced technical

© Глазовский В.В., 2025

training. The author also develops a classification of software tools used by perpetrators in social engineering attacks, based on their functional purpose and intended use. Special attention is devoted to mechanisms for counteracting this type of crime. The results of the study enable the development of practical recommendations for law enforcement agencies aimed at identifying offenders through the analysis of geolocation data and VPN traffic.

Keywords: social engineering, offender personality, cybercrime, cybersecurity, information and telecommunication technologies, software tools, forensic science, operational investigative activities

For citation: Glazovsk V.V. Social engineering in the digital age: criminal personality analysis and software tool classification // Truth and law. 2025. № 3(33). P. 106–114.

В современную эпоху цифровой глобализации методы социальной инженерии становятся одним из наиболее опасных и распространенных способов совершения преступлений. Указанная категория преступлений направлена на получение конфиденциальной информации, несанкционированного доступа к ресурсам, а также на побуждение жертвы совершить те или иные действия в интересах преступника. Термин социальная инженерия раскрывается в «Основных направлениях развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов», одобренных советом директоров Банка Российской Федерации, и представляет собой введение в заблуждение путем обмана или злоупотребления доверием для получения несанкционированного доступа к информации, электронным средствам платежа или побуждения владельцев самостоятельно совершить перевод денежных средств с целью их хищения[1]. По сообщению Генерального прокурора Российской Федерации И.В. Краснова, в 2024 г. количество преступлений в сфере информационно-коммуникационных технологий увеличилось на 13 %, а две трети из указанного количества – более 485 тысяч преступлений – составили хищения, совершаемые с применением социальной инженерии[2]. Рост количества преступлений, совершенных с использованием методов социальной инженерии, и увеличение степени вреда, причиняемого общественным отношениям в результате совершения данного вида преступлений, порождает необходимость в исследовании данного явления и обуславливает его актуальность.

В статье приведен криминологический анализ личности преступника, совершающего преступления с применением методов социальной инженерии, разработана классификация программного обеспечения, используемого преступниками в качестве инструментов при совершении данной категории преступлений, а также исследован функционал указанных программных инструментов.

Проведенное исследование способствует формированию эффективных мер противодействия преступлениям, основанным на манипуляциях сознанием людей, и повышению уровня цифровой безопасности общества. Результаты проведенного исследования могут быть использованы сотрудниками правоохранительных органов на практике, а также являться основой для проведения дальнейших научных изысканий в сфере безопасности в информационно-телекоммуникационных технологий.

Анализируя психологические особенности личности преступника, совершающего преступления с применением методов социальной инженерии, стоит отметить, что знание отдельных качеств личности данной категории преступников позволяет предугадать их линию поведения, а также успешно пресекать их действия до достижения ими желаемого преступного результата.

Справедливо отмечают Н.И. Старостенко и А.Ю. Головин, что профессиональные преступники, совершающие преступления с применением методов социальной инженерии, практически в каждом случае являются хорошими

[1] Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023–2024 годов. Доступ из информ.-правовой системы «Гарант».

[2] ТАСС: информ. агентство России. URL: https://tass.ru/ekonomika/23316771 (дата обращения: 13.05.2025).

и подготовленными манипуляторами, прошедшими соответствующее обучение по обретению криминальных навыков обмана, манипулирования, запугивания и убеждения [1]. Зачастую злоумышленник обучается молниеносно находить подходящий ответ на те или иные каверзные вопросы со стороны его собеседника, что еще больше вводит в заблуждение его потенциальную жертву. Преступники, совершающие рассматриваемую категорию преступлений, также обучаются эффективному установлению психологического контакта с людьми, имеют поставленную речь, обучаются владению специализированной терминологией в зависимости от изображаемой ими роли и преступной легенды, имеют широкое представление о спектре возможностей использования социальных сетей и особенностях дистанционного банковского обслуживания.

Также стоит отметить гибкое обращение преступников с методами психологического манипулирования над потенциальными жертвами. Ключевыми эмоциями, на которые прежде всего направлены действия злоумышленников, является чувство доверия, чувство страха и чувство срочности. Злоумышленник обманным путем входит в доверительные отношения к жертве, налаживая с ней психологический контакт, затем вселяет в нее чувство страха посредством угрозы наступления возможных негативных последствий для жертвы в случае, если она откажется поступать так, как ей велит злоумышленник, после чего преступник вызывает у жертвы чувство срочности, создавая ощущение необходимости срочно совершить то или иное действие по указанию злоумышленника в целях избегания ранее озвученных негативных последствий. Мнимое отсутствие времени для обдумывания решения заставляет жертву действовать незамедлительно, не руководствуясь при этом логикой и здравым смыслом, что позволяет преступнику достичь желаемого результата.

Также следует учесть, что успешность применения техник социальной инженерии при совершении преступлений зачастую зависит от подготовительного этапа [2], в связи с чем можно сделать вывод о том, что преступники, совершающие данную категорию преступлений, зачастую обладают высокими навыками по сбору информации о потенциальной жертве, владеют техниками OSINT (open source intelligence – разведки по открытым источникам), имеют хорошие навыки использования компьютеризированной техники и интернет-технологий, обладают умениями по созданию фишинговых (поддельных) интернет-ресурсов, копирующих официальные сайты известных интернет-площадок или социальных сетей, обладают умениями по использованию вредоносного программного обеспечения, нейросетей, графических и аудио и видеоредакторов в целях осуществления подделок фотографий, а также технологий «deepfake», позволяющих сфальсифицировать видеоизображение и голос другого человека.

Проведенным анализом программного обеспечения, используемого злоумышленниками при совершении преступлений с применением методов социальной инженерии, автором предлагается следующая классификация указанных программных инструментов: маскирующее программное обеспечение; вредоносное программное обеспечение; программное обеспечение удаленного доступа; программное обеспечение, предназначенное для рассылки спама.

К категории маскирующего программного обеспечения можно отнести программы, позволяющие осуществить маскировку следов преступной деятельности злоумышленника, подменить абонентский номер мобильного телефона или ip-адрес, используемый преступником. К данному виду программного обеспечения относится массивный пласт программ, среди которых можно выделить программное обеспечение, используемое для «спуфинга» (подмены) абонентского номера при осуществлении звонков: «SpoofCard», «SpoofTel», «Bluff My Call», «Fake Call & SMS», «Dingtone», «3CX», «FreePBX», «ZoiPer». Гайдин А.И., Звягин И.С. и Садырин И.С. также упоминают о таких общедоступных программах, как «Smiddle Smart SIP Proxy», «Sipcaller», «Foxycall» и «Black Wolf» [3]. Указанные программные средства

предназначены для изменения, модификации идентификатора вызывающего абонента – параметра «Caller ID», используемого в SIP-телефонии. Параметр «Caller ID» позволяет абонентам идентифицировать входящие вызовы, прежде чем ответить на них. Данный параметр может содержать как номер телефона вызывающего абонента, так и различные комбинации букв и символов.

Используя данное программное обеспечение, злоумышленник может осуществить изменение параметра «Caller ID», заменив свой абонентский номер, который отображается при звонке другому человеку, на любой другой абонентский номер, либо на слово или фразу, на которую будет заменен данный параметр. Изменив данный параметр, при звонке на телефоне жертвы абонентский номер злоумышленника может определяться иначе, в том числе для большего убеждения своей жертвы злоумышленник может изменить отображение своего абонентского номера на телефоне жертвы названием банка или правоохранительного органа, например: Сбербанк или ФСБ России.

При этом стоит отметить, что в случае изменения параметра «Caller ID», определить настоящий абонентский номер, используемый злоумышленником, является крайне сложной задачей. Зачастую злоумышленники, наряду с использованием вышеуказанного программного обеспечения, используют абонентские номера – «дропы», то есть сим-карты, зарегистрированные на третьих лиц, которые в большинстве случаев даже не подозревают, что их абонентский номер может использоваться кем-то в преступных целях.

При изменении параметра «Caller ID» абонентский номер злоумышленника также будет отображаться в детализации телефонных соединений в измененном виде, что существенно затруднит идентификацию реального номера преступника и его деанонимизацию. Это связано с тем, что информация о параметре «Caller ID» передается вместе с сигналом вызова и фиксируется в журнал оператора в том виде, в котором она была изменена.

По схожей технологии работает программа с наименованием «TipTopSMSWin», предназначенная для подмены абонентского номера при отправке СМС-сообщений.

Вместе с тем существует несколько способов противодействия противоправной модификации параметра «Caller ID», позволяющих определить или проверить подлинность номера. К ним можно отнести: системы безопасности операторов, автоматически определяющие и блокирующие подмену абонентского номера; анализ трафика, благодаря которому существует возможность определения источника вызова и проверки изменения параметра «Caller ID»; технологии проверки подлинности, позволяющие осуществить проверку подлинности «Caller ID». Также стоит упомянуть и запущенную в декабре 2022 г. Роскомнадзором платформу верификации телефонных вызовов «Антифрод». Данная платформа верификации получает информацию обо всех телефонных звонках, при этом операторы сотовой связи, в свою очередь, в автоматическом режиме запрашивают и получают данные об активности и подлинности телефонного номера абонента, осуществившего звонок. В случае если система «Антифрод» подтверждает, что вызов реальный и абонентский номер не является подменным, устанавливается безопасное соединение. В противном случае, если такого подтверждения нет, подозрительный вызов блокируется оператором сотовой связи[3].

По данным Роскомнадзора, оглашенным на форуме «Спектр 2024», платформа верификации «Антифрод» за девять месяцев 2024 г. успешно заблокировала 577 млн телефонных звонков злоумышленников, благодаря чему доля преступлений, совершаемых с использованием подмены абонентского номера, уменьшилась с 30 до 2 %[4].

[3] Центр мониторинга и управления сетью связи общего пользования. URL: https://portal.noc.gov.ru/ru/news/2023/11/27/o-funkcionirovanii-sistemy-antifrod/ (дата обращения: 14.05.2025).
[4] Интерфакс: информ. группа. URL: https://www.interfax.ru/russia/988120 (дата обращения: 14.05.2025).

К маскирующему программному обеспечению также можно отнести программу «Call Voice Changer – IntCall» и ее аналоги. Данное программное обеспечение предназначено для изменения голоса звонящего человека в режиме реального времени в ходе телефонного разговора. Инструментарий данного программного обеспечения позволяет модифицировать высоту и тембр голоса звонящего человека, изменив его практически до неузнаваемости. Существуют случаи, при которых злоумышленник мог подделать параметры голоса знакомого или родственника потенциальной жертвы, в целях наиболее успешного применения методов социальной инженерии, создания иллюзии доверия или авторитета для жертвы.

В настоящее время в научном сообществе ведутся дискуссии относительно законодательного установления обязательной фоноскопической регистрации граждан в целях предупреждения и выявления преступлений, совершенных с использованием средств телефонной связи. Так, В.С. Кашпоровой предлагается разработка и принятие федерального закона о государственной фоноскопической регистрации в Российской Федерации и сборе на его основании фоноскопической информации граждан [4]. Вместе с тем в современных условиях предлагаемые В.С. Кашпоровой меры, вероятно, не принесут желаемого результата, ввиду наличия в свободном доступе программного обеспечения, предназначенного для изменения фоноскопических параметров голоса вызывающего абонента.

Также в качестве маскирующего программного обеспечения злоумышленники могут использовать различные VPN (virtual private network – виртуальная частная сеть) сервисы. Данные сервисы предназначены для установления анонимного интернет-соединения между устройством пользователя и удаленным сервером. Без использования VPN-сервиса весь трафик пользователя проходит через сервер интернет-провайдера, который позволяет идентифицировать своего пользователя посредством обозначения его уникального числового идентификатора устройства в компьютерной сети – IP-адреса. При использовании VPN-сервиса весь интернет-трафик пользователя направляется не через сервер конкретного интернет-провайдера, а в собственные частные серверы VPN-сервиса, в связи с чем IP-адрес пользователя меняется на местоположение VPN-сервера. Популярностью среди преступников пользуются такие VPN-сервисы, как «ExpressVPN», «NordVPN», «Private Internet Access», «IPVanish», «CyberGhost» и др. Вместе с тем стоит отметить, что использование VPN-сервисов преступниками не во всех случаях позволяют полностью анонимизировать их действия. Ряд VPN-сервисов могут использовать политику ведения журналов, то есть своего рода собирать и хранить данные о пользователе, использующем данный сервис посредством записи информации о настоящем IP-адресе пользователя, объеме переданных данных и посещенных сайтах. Подобного рода сервисы в силу закона обязаны предоставить по запросу правоохранительных органов имеющуюся у них информацию о пользователе, в том числе и его настоящий IP-адрес, при установлении которого определить местонахождение злоумышленника не составит сложности. Ряд VPN-сервисов не осуществляют ведение подобного рода «журналов», что существенно затрудняет возможность деанонимизации преступника, использующего подобный сервис.

Существует несколько способов для установления местонахождения преступника, использующего VPN-сервисы. Так, в случае если злоумышленник совершает преступление с применением VPN-сервиса, используя мобильное устройство, его точное местонахождение может быть установлено путем использования метода триангуляции по базовым станциям, то есть метода определения местоположения мобильного устройства с использованием сигналов от нескольких базовых станций. Таким образом, информация о позиционировании мобильного устройства при интернет-сессиях сохраняется у оператора сотовой связи. При сопоставлении зон покрытия трех базовых станций, по которым позиционируется мобильное устройство злоумышленника, появляется возможность определения его наиболее точного местоположения. Используя данные операторов

сотовой связи о позиционировании мобильного устройства злоумышленника, а также данные о расстояниях от трех или более базовых станций, можно построить геометрическую модель, например круги или треугольники, обозначающие зоны покрытия базовых станций, в которых будет находиться мобильное устройство. Пересечение областей всех трех базовых станций указывает на наиболее точное местоположение устройства злоумышленника. При применении преступником VPN-сервисов на стационарном устройстве определить его фактический IP-адрес можно посредством глубокого анализа динамики изменений его IP-адреса в ходе использования VPN-сервиса. Так, в случае если правоохранительным органам известны идентификационные сведения о странице социальной сети, которая находится в пользовании преступника (интернет-адрес, наименование, id и т.д.), у сотрудников следственных и оперативных подразделений появляется возможность запроса сведений у владельцев соответствующих интернет-ресурсов об IP-адресах, с которых осуществлялся вход или использование интересующих правоохранительные органы страниц пользователей. Посредством анализа массива полученной информации существует возможность отграничения IP-адресов VPN-сервисов и IP-адреса, который с наибольшей долей вероятности может являться фактическим IP-адресом злоумышленника. Стоит также отметить, что далеко не все VPN-сервисы предоставляют постоянное и стабильное интернет-соединение через собственные серверы. Зачастую подключение к частным серверам может обрываться, и в такие моменты фактический IP-адрес злоумышленника фиксируется его интернет-провайдером. В подобных ситуациях следственным и оперативным подразделениям важно заметить подобный сбой подключения злоумышленника к VPN-сервису и обнаружить существенную разницу в смене его IP-адреса, что может выражаться в резкой смене IP-адреса с сервера, расположенного в иностранном государстве, на сервер интернет-провайдера, находящегося в Российской Федерации.

К программному обеспечению, предназначенному для рассылки спама, можно, прежде всего, отнести программы, предназначенные для массовой рассылки СМС-сообщений и электронных писем, такие как: «SMSBomba», «SmsTool», «TipTopSMSWin», «ePochta Mailer», «UniSender», «SendPulse» и многие другие. Подобного рода программы зачастую используются для фишинговых атак и массовой рассылки текстовых сообщений, которые в том числе могут содержать в себе ссылки на вредоносные интернет-ресурсы, при переходе на которые запускаются скрипт установки вредоносного программного обеспечения. Используя данное программное обеспечение в синтезе с приемами социальной инженерии, злоумышленники могут отправлять сообщения, представляясь сотрудниками банка, правоохранительных органов или даже родственниками потенциальных жертв, побуждая их переходить по вредоносным интернет-ссылкам, осуществлять переводы денежных средств либо совершать иные действия, выгодные злоумышленникам.

Массовая СМС-атака с использованием указанного программного обеспечения может также служить в качестве фильтрующего этапа при использовании приема «претекстинга». Под «претекстингом» понимается прием социальной инженерии, представляющий собой совершение мошеннических действий, осуществляемых преступником с использованием средств мобильной связи по заранее подготовленному тексту (сценарию), целью которого является совершение потенциальной жертвой действий в интересах злоумышленника, либо получение конфиденциальной информации, необходимой для хищения денежных средств потерпевшего [5].

В качестве примера комбинирования приема «претекстинга» с использованием массовой СМС-атаки можно привести следующую преступную схему. На первоначальном этапе злоумышленником осуществляется массовая рассылка спама, путем направления СМС-сообщений 100 различным абонентам. Текст сообщения построен преступником таким образом, что оно выглядит как уведомление о взломе страницы социальных сетей, порталов государственных услуг либо как уведомление о списании денежных средств с банковского счета. При этом текст

сообщения обязательно содержит контактный абонентский номер либо интернет-ссылку, куда потенциальной жертве следует обратиться для «защиты» своих персональных данных или денежных средств от мошенников. Из 100 абонентов, которым было адресовано сообщение указанного типа, часть людей обязательно перейдет по прикрепленной интернет-ссылке или позвонит по указанному в подобного рода сообщении номере. После того, как потенциальная жертва совершит данные действия, злоумышленник начнет следующий этап своей работы, непосредственно вступая с «попавшейся» жертвой в диалог, в соответствии с ранее разработанным преступным сценарием.

Программы для удаленного доступа используются злоумышленниками для получения несанкционированного доступа к управлению техническим устройством жертвы. Подобного рода программное обеспечение позволяет удаленно получать доступ к личной информации, хранящейся на устройстве жертвы и совершать мошеннические операции. К наиболее популярным программам удаленного доступа относятся: «AnyDesk», «TeamViewer», «AeroAdmin», «Rustdesk», «HopToDesk».

Учитывая, что указанное программное обеспечение пользуется широким спросом у специалистов технической поддержки крупных организаций, злоумышленники, зачастую используя приемы социальной инженерии, вступают в контакт с жертвой сотрудником какой-либо крупной организации и представляются специалистом технической поддержки, затем под предлогом устранения той или иной неисправности или пробела в защите, предлагают жертве установить на его устройство программное обеспечение, предназначенное для удаленного доступа. По окончании установки указанного программного обеспечения оно генерирует уникальный код доступа, который необходим преступнику для возможности удаленного подключения к устройству жертвы и управления этим устройством. После получения данного уникального кода и доступа к устройству жертвы злоумышленник имеет возможность открывать банковские приложения, приложения различных интернет-магазинов, получить полную информацию о банковских картах, сведения, необходимые для авторизации на тех или иных интернет-ресурсах, а также сведения личного характера, хранящиеся на техническом устройстве жертвы.

В целях противодействия преступникам, использующим программное обеспечение, предназначенное для удаленного доступа, следует не устанавливать какие-либо программы по просьбе малознакомых лиц, использовать антивирусное программное обеспечение с функцией защиты от удаленного доступа, а также использовать двухфакторную аутентификацию, позволяющую предотвратить несанкционированный доступ злоумышленников к тем или иным конфиденциальным данным и интернет-ресурсам.

К самостоятельной отдельной категории программного обеспечения, используемого злоумышленниками при совершении преступлений с применением методов социальной инженерии, можно отнести инструменты и программное обеспечение технологии deepfake.

Как упоминалось ранее, технология deepfake позволяет преступникам сфальсифицировать видеоизображение и голос конкретного человека, в связи с чем использование данной технологии в синтезе с применением методов социальной инженерии сильно повышает эффективность подобных атак.

К основным и наиболее популярным программам и инструментам технологии deepfake можно отнести «DeepFaceLab» – программное обеспечение, позволяющее создавать дипфейки высокого качества, «Zao» – программа, предназначенная для замены лиц в видеозаписях, а также различные онлайн-сервисы, находящиеся в открытом доступе сети Интернет, позволяющие создавать высококачественные дипфейки пользователями, которые не имеют специальных навыков программирования.

В настоящее время, учитывая участившиеся факты применения технологии deepfake, Следственный комитет Российской Федерации выступил с инициативой дополнения ст. 63 Уголовного кодекса Российской Федерации[5] новым отягчающим обстоятельством, связанным с использованием при совершении преступления информационно-телекоммуникационных технологий, включая технологии искусственного интеллекта[6]. Представляется, что подобное дополнение законодательства благоприятно скажется на криминогенной обстановке и уровне преступлений, совершаемых с использованием технологии deepfake.

Особое внимание также следует уделить способам распознавания видеозаписей, созданных с использованием технологии deepfake. Как правило, подобные видеозаписи имеют ряд часто встречающихся «графических артефактов», среди которых можно выделить: неправдоподобные глаза, неестественный тон кожи, неверное отображение рук человека, неверное количество пальцев на руках, отсутствие синхронизации между речью человека и движением губ на видеозаписи. Однако не стоит забывать, что нейросети продолжают совершенствоваться и на сегодняшний день все чаще встречаются высококачественные deepfake видеозаписи, распознать которые зачастую бывает затруднительно.

Рассмотренное выше программное обеспечение, как правило, свободно распространяется в интернет-пространстве и доступно каждому пользователю. Несмотря на то, что указанные программы предназначены для выполнения тех или иных легальных задач, злоумышленники умело приспосабливают их в инструменты для совершения своих противоправных действий в киберпространстве.

В заключении стоит отметить, что жертвами преступлений, совершаемых с применением методов социальной инженерии, наиболее часто становятся пенсионеры и люди предпенсионного возраста, а также иные граждане, не обладающие достаточными познаниями в области цифровой грамотности. В связи с этим представляется целесообразным внедрение обучения цифровой грамотности и ее популяризация среди всех слоев общества, а также повсеместное освещение в кругах общественности актуальных цифровых угроз и приемов социальной инженерии, используемых преступниками. Кроме того, представляется целесообразным ужесточить меры противодействия анонимизации личности в сети Интернет и при использовании информационно-телекоммуникационных технологий, запретив свободное распространение VPN-сервисов, использующих политику «без журналов», блокировав возможность модификации параметра «Caller ID» в SIP-телефонии, а также введя юридическую ответственность за продажу чужих абонентских номеров или банковских счетов.

Проведенное исследование способствует углублению понимания психологических и технических аспектов преступлений с применением методов социальной инженерии, что может повысить эффективность профилактики и расследования правонарушений данного вида. Результаты работы могут иметь практическую значимость для правоохранительных органов и специалистов в области кибербезопасности, предлагая комплексный подход к выявлению и противодействию новым видам преступной деятельности в цифровую эпоху.

Список источников

1. Старостенко Н.И. Криминалистическая характеристика личности преступника, совершающего хищения с применением методов социальной инженерии // Вестник Краснодарского университета МВД России. 2022. № 4(58). С. 89–95.

[5] Уголовный кодекс Рос. Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 31 июля 2025 г.; с изм. и доп., вступ. в силу с 1 сент. 2025 г.). Доступ из справ.-правовой системы «КонсультатнПлюс».

[6] ТАСС: информ. агентство России. URL: https://tass.ru/obschestvo/23706779 (дата обращения: 14.05.2025).

2. Старостенко Н.И. Криминалистические особенности способов совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета. Право 1. 2024. Т. 15. Вып. 1. С. 152–170.

3. Гайдин А.И., Звягин И.С., Садырин И.С. Механизм хищений денежных средств, совершаемых с использованием технологий IP-телефонии и программ подмены номеров // Вестник Воронежского института МВД России. 2022. № 3. С. 202–207.

4. Кашпорова В.С. Обязательная фоноскопическая регистрация как способ снижения количества совершаемых телефонных мошенничеств // Вестник Белгородского юридического института МВД России им. И.Д. Путилина. 2024. № 3. С. 80–85.

5. 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.

References

1. Starostenko N.I. Kriminalisticheskaya harakteristika lichnosti prestupnika, sovershayushchego hishcheniya s primeneniem metodov social'noj inzhenerii // Vestnik Krasnodarskogo universiteta MVD Rossii. 2022. № 4(58). S. 89–95.

2. Starostenko N.I. Kriminalisticheskie osobennosti sposobov sovershheniya hishchenij s primeneniem metodov social'noj inzhenerii i informacionno-telekommunikacionnyh tekhnologij // Vestnik Sankt-Peterburgskogo universiteta. Pravo 1. 2024. T. 15. Vyp. 1. S. 152–170.

3. Gajdin A.I., Zvyagin I.S., Sadyrin I.S. Mekhanizm hishchenij denezhnyh sredstv, sovershaemyh s ispol'zovaniem tekhnologij IP-telefonii i programm podmeny nomerov // Vestnik Voronezhskogo instituta MVD Rossii. 2022. № 3. S. 202–207.

4. Kashporova V.S. Obyazatel'naya fonoskopicheskaya registraciya kak sposob snizheniya kolichestva sovershaemyh telefonnyh moshennichestv // Vestnik Belgorodskogo yuridicheskogo instituta MVD Rossii im. I.D. Putilina. 2024. № 3. S. 80–85.

5. Zotina E.V. Pretekstinq kak priyom social'noj inzhenerii, ispol'zuemyj telefonnymi moshennikami: kriminologicheskij vzglyad na problemu // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2022. T. 13. № 4(50). S. 93–99.

Статья поступила в редакцию 23.06.2025; одобрена после рецензирования 21.07.2025; принята к публикации 23.07.2025.
The article was submitted 23.06.2025; approved after reviewing 21.07.2025; accepted for publication 23.07.2025.

Информация об авторе
В.В. Глазовский – аспирант Санкт-Петербургской академии Следственного комитета (Россия, 190000, г. Санкт-Петербург, наб. р. Мойки, 96); следователь по особо важным делам первого отдела по расследованию особо важных дел (о преступлениях прошлых лет) следственного управления Следственного комитета Российской Федерации по Калужской области (Россия, 248000, г. Калуга, ул. Салтыкова-Щедрина, 107/103).

Information about the author
V.V. Glazovsky – graduate student of the SK RF SPb Academy (Russia, 190000, St. Petersburg, nab. r. Moika, 96); Senior Investigator for Particularly Important Cases First Division for the Investigation of Particularly Important Cases (on Crimes of Past Years) Investigative Department of the Investigative Committee of the Russian Federation for the Kaluga Region (Russia, 248000, Kaluga, Saltykova-Shchedrina Street, 107/103).