Научная статья
УДК 343.3
doi: 10.33463/2687-122X.2025.20(1-4).2.294-307

# ПРИЕМЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В АРСЕНАЛЕ ПРЕСТУПНИКОВ: УГЛУБЛЕННЫЙ АНАЛИЗ МЕТОДОВ И АКТУАЛЬНЫХ УГРОЗ

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

**Аннотация.** Тема методов социальной инженерии, применяемых преступниками, является крайне актуальной в контексте обеспечения кибербезопасности в современных условиях. Социальная инженерия представляет собой совокупность психологических методов, используемых злоумышленниками для манипулирования людьми, получения от них необходимой преступникам информации или выполнения тех или иных выгодных злоумышленнику действий. Данная область преступной деятельности стала особенно распространенной с развитием информационно-телекоммуникационных технологий, что привело к значительному увеличению количества преступлений в киберпространстве. Рост числа киберпреступлений, совершаемых с применением методов социальной инженерии, требует активного развития мер по их предотвращению и борьбе с ними. Это включает в себя не только решения технического характера, но и психологические аспекты, поскольку основным объектом атаки преступников, совершающих преступление с использованием методов социальной инженерии, являются эмоции людей и уязвимости в их психике. Статья посвящена анализу методов социальной инженерии, используемых преступниками в современных условиях, что позволяет глубже понять механизмы, лежащие в основе социальной инженерии, и разработать эффективные меры по защите от таких угроз. Понимание методов, используемых преступниками, имеет решающее значение для разработки контртехнологий, направленных на формирование психологической защищенности граждан и повышение их устойчивости к методам социальной инженерии. В статье рассмотрены основные нормативные и научные подходы к определению понятия социальной инженерии, приводятся криминологические характеристики личности преступника, совершающего преступления указанной категории, классификация основных приемов социальной инженерии, используемых преступниками, таких как фишинг, претекстинг, кви про кво и другие, обозначены актуальные пробле-

мы в сфере обеспечения кибербезопасности. В работе также проведен анализ наиболее актуальных преступных схем, используемых злоумышленниками при совершении преступлений с применением методов социальной инженерии. Результаты проведенного исследования могут служить основой для дальнейших научных изысканий в области противодействия киберпреступности и формирования эффективных механизмов защиты от манипулятивных технологий.

**Ключевые слова:** социальная инженерия, методы социальной инженерии, претекстинг, кибербезопасность, киберпреступления, интернет-угрозы, информационно-телекоммуникационные технологии, криминалистика, оперативно-розыскная деятельность

**Для цитирования**
Глазовский В. В. Приемы социальной инженерии в арсенале преступников: углубленный анализ методов и актуальных угроз // Уголовно-исполнительное право. 2025. Т. 20(1–4), № 2. С. 294–307. DOI: 10.33463/2687-122X.2025.20(1-4).2.294-307.

Original article

# SOCIAL ENGINEERING TECHNIQUES IN THE ARSENAL OF CRIMINALS: AN IN-DEPTH ANALYSIS OF METHODS AND CURRENT THREATS

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

**Abstract.** The topic of social engineering methods used by criminals is extremely relevant in the context of cybersecurity in modern conditions. Social engineering is a set of psychological methods used by attackers to manipulate people, obtain information from them that criminals need, or perform certain actions beneficial to the attacker. This area of criminal activity has become especially widespread with the development of information and telecommunication technologies, which has led to a significant increase in the number of crimes in cyberspace. The growing number of cybercrimes committed using social engineering methods requires the active development of measures to prevent and combat them. This includes not only technical solutions, but also psychological aspects, since the main target of attack by criminals who commit crimes using social engineering methods are people's emotions and vulnerabilities in their psyche. This article is devoted to an in-depth analysis of social engineering methods used by criminals in modern conditions. The analysis of these methods allows for a deeper understanding of the mechanisms underlying social engineering and the development of effective measures to protect against such threats. Understanding the methods used by criminals is crucial for developing counter-technologies aimed at creating psychological security for citizens and increasing their resistance to social engineering methods. This article examines the main

regulatory and scientific approaches to defining the concept of social engineering, provides criminological characteristics of the personality of a criminal who commits crimes of this category, a classification of the main social engineering techniques used by criminals, such as phishing, pretexting, qui pro quo and others, identifies current problems in the field of cybersecurity. The paper also analyzes the most relevant criminal schemes used by intruders when committing crimes using social engineering methods. The results of the conducted research can serve as the basis for further scientific research in the field of countering cybercrime and the formation of effective protection mechanisms against manipulative technologies.

**Keywords:** social engineering, social engineering methods, pretexting, cybersecurity, cybercrime, Internet threats, information and telecommunication technologies, criminalistics, operational investigative activities

**For citation**

Glazovsky, V. V. 2025, 'Social engineering techniques in the arsenal of criminals: an in-depth analysis of methods and current threats', *Penal law,* vol. 20(1–4), iss. 2, pp. 294–307, doi: 10.33463/2687-122X.2024.20(1-4).2.294-307.

В современных реалиях информационно-телекоммуникационные технологии стали неотъемлемой частью жизни каждого человека, а также всех сфер деятельности общества и государства. Внедрение информационных технологий благоприятно влияет на развитие информационного общества, способствует экономическому развитию государства, а также облегчает решение задач по оперативному обмену информацией между пользователями. Вместе с тем следует отметить, что с развитием информационных технологий и их повсеместным внедрением во все сферы социальной действительности возникли новые формы и модели совершения общественно опасных деяний с использованием информационных технологий и информационно-телекоммуникационной сети Интернет. Совершенствование способов и методов противодействия киберпреступности, разработка специализированного программного обеспечения, предназначенного для идентификации личности преступника и его местонахождения, борьбы с вредоносными программами, а также применяемые меры по снижению уровня виктимности населения влекут за собой разработку преступниками новых, потенциально опасных методов совершения преступлений в сети Интернет, способных обойти современные системы защиты и причинить существенный вред жертве преступления, обществу и государству.

Одну из наиболее существенных угроз в эру глобальной информационализации общества представляют собой преступления, совершаемые с применением методов социальной инженерии.

В настоящее время в научной среде отсутствует единообразное понимание сущности социальной инженерии и данная категория толкуется каждым автором по-разному. Так, В. В. Суворова и Л. А. Суворова определяют социальную инженерию как вид совершения компьютерных преступлений, направленных на несанкционированное получение информации путем использования слабых мест в психике человека, к которым относятся инициативность, нервно-психическая слабость, чувствительность и др. [4]. По мнению Е. В. Зотиной, социальная инженерия – это особый нетехнический способ получения преступником конфиденциальной информации, основанный на коммуникативном взаимодействии между людьми [5]. Н. И. Старостенко приводит более

лаконичное определение социальной инженерии как криминалистической категории и определяет ее как приемы обмана и психологического манипулирования людьми в целях осуществления контроля за их поведением или действиями [1]. Анализируя данные научные подходы, можно констатировать, что социальная инженерия как криминалистическая категория содержит в себе следующие признаки: коммуникационный характер действий, поскольку методы социальной инженерии предполагают общение и взаимодействие между преступником и его потенциальной жертвой; направленность данных действий на получение конфиденциальных сведений; применение методов оказания психологического воздействия и манипулирования собеседником; достижение цели преступной деятельности путем обмана или злоупотребления доверием; информационное пространство как зона деятельности киберпреступников; корыстный мотив или иная личная заинтересованность преступников.

Стоит также отметить, что законодательное определение криминалистической категории социальной инженерии в настоящее время отсутствует, однако существует его нормативное толкование, которое закреплено в таком документе, как «Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов». В указанном правовом акте неоднократно упоминается категория социальной инженерии, а также приводится ее нормативное определение, согласно которому под социальной инженерией понимается 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].

В ходе анализа методов социальной инженерии заслуживает внимания точка зрения Н. И. Старостенко о том, что методы социальной инженерии, применяемые преступниками, не являются способами совершения преступления, а лишь выступают элементом способа совершения преступления в механизме преступной деятельности [3].

Анализ научных трудов по исследуемой проблематике показал недостаточную углубленность классификации приемов социальной инженерии, используемых преступниками при совершении преступлений. Так, Е. В. Зотина в научных публикациях упоминает такие приемы, как «фишинг (вишинг)», «претекстинг», «дорожное яблоко», «кви про кво», «троянский конь» [5]. Н. И. Старостенко добавляет к указанным приемам шантаж [2], а М. О. Янгаева упоминает приемы «обратная социальная инженерия» и «вымогатель» [8], однако они не в полной мере отражают весь спектр актуальных киберугроз.

На наш взгляд, приемы социальной инженерии, используемые преступниками для достижения преступной цели, условно можно классифицировать: на приемы, совершаемые с использованием вредоносного программного обеспечения, к которым можно отнести такие приемы, как «дорожное яблоко», «троянский конь», «scareware (пугалка)», «rogueattack (мошенническая атака)», «baiting (приманка)», «water-holling (водопой)»; приемы, совершаемые с использованием телефонных и иных переговоров с жертвой: «вишинг (voisephishing – голосовой фишинг)», «смишинг (smishing – смс-фишинг)», «претекстинг», «кви про кво (от лат. *quidproquoc* – услуга за услугу)», «honeytrap (медо-

[1] См.: Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023–2024 годов // Гарант.ру. Информационно-правовой портал : сайт. URL: https://www.garant.ru (дата обращения: 02.02.2025).

вая ловушка)»; комбинированные приемы, сочетающие в себе признаки двух вышеуказанных категорий, к которым можно отнести такой прием социальной инженерии, как «клон-фишинг».

Следует отметить, что некоторые из перечисленных приемов социальной инженерии имеют заметное сходство друг с другом. Для более детального понимания их отличий необходимо провести анализ каждого из указанных приемов, основанный на личном опыте, данных специализированной литературы, а также судебной практики.

Суть такого приема социальной инженерии, как «дорожное яблоко», состоит в получении злоумышленником конфиденциальной информации посредством самостоятельного внедрения жертвой в используемое им личное компьютеризированное оборудование вредоносных программ. Таким образом, злоумышленником подготавливается носитель информации, который используется им в дальнейшем в качестве приманки. Подобным носителем информации может служить USB-флеш-накопитель, карта памяти, компакт-диск, жесткий диск и т. д. На подготовленный носитель информации злоумышленником предустанавливается вредоносное программное обеспечение, которое часто направлено на сбор и передачу конфиденциальной информации в руки злоумышленника. После этого подготовленный носитель информации, содержащий вредоносное программное обеспечение, злоумышленник оставляет в общественном месте либо в помещениях различных организаций, а также в зданиях органов государственной власти. В зависимости от зоны расположения такой «ловушки» злоумышленники часто наносят на оставленный ими накопитель информации логотип или эмблему организации, где он был оставлен, а также интригующий текст, например: «график выплаты заработной платы», «приказ о поощрении и выплате премии» и подобные тексты, направленные на побуждение чувства любопытства у потенциальной жертвы [7]. Заинтересовавшийся человек, обнаружив подобную «ловушку», из любопытства может решить открыть и запустить обнаруженный им накопитель информации на личном или рабочем компьютере, после чего установленное на данном накопителе информации вредоносное программное обеспечение незамедлительно начнет свою работу. Стоит отметить, что потенциальная жертва может даже не подозревать о наличии в найденном им накопителе информации вредоносных программ, поскольку нередко они могут быть скрытыми. При применении приема «дорожное яблоко» злоумышленниками наиболее часто используются программы кейлоггеры – «клавиатурные шпионы», то есть программное обеспечение, фиксирующее каждое нажатие пользователя на клавиатуру и мышь и сохраняющее эту информацию в текстовом документе, который в дальнейшем передается злоумышленнику посредством сети Интернет. Программы кейлоггеры практически в каждом случае используются в паре с вредоносным программным обеспечением, направленным на удаление сохраненного на персональном компьютере кеша. Таким образом, при удалении хранящегося в памяти персонального компьютера кеша у пользователя возникает необходимость в повторной авторизации на различных сайтах, в социальных сетях, личных кабинетах, а также в повторном введении данных своей банковской карты при совершении покупок в сети Интернет. Введенные пользователем логины и пароли при авторизации, а также данные банковской карты при помощи программы кейлоггера сохраняются и передаются в руки злоумышленнику, предоставляя ему доступ к персональным данным и иным конфиденциальным сведениям. Вместе с тем гораздо большую опасность представляют так называемые бэкдор-программы (от англ. *backdoor* – черный ход), суть которых заключается в незаметном встраивании

в сервер или операционную систему устройства и предоставлении удаленного доступа к персональному компьютеру третьему лицу.

Прием «троянский конь» имеет заметную схожесть с «дорожным яблоком». По своей сути, прием «дорожное яблоко» является разновидностью «троянского коня». В обоих случаях злоумышленником осуществляется принудительная установка на устройство потенциальной жертвы вредоносного программного обеспечения. Прием «троянский конь» состоит в отправке жертве электронного письма или сообщения, которое может заинтересовать и побудить чувство любопытства у своей жертвы. Нередко данное письмо может содержать информацию о необходимости установления новых обновлений важных программ либо о распродаже в том или ином магазине, получении «подарка» с обязательным прикреплением к такому письму интернет-ссылки для перехода на сайт загрузки обновления, получения скидки или подарка. После перехода по данной интернет-ссылке вместо получения ожидаемого подарка или обновления программного обеспечения жертву ожидает лишь установка вредоносных программ на используемый персональный компьютер. При этом вредоносная программа может быть замаскирована под файл безвредной, например антивирусной, при запуске установки которой вредоносное программное обеспечение проникает в файловую систему компьютера.

Как правило, подобного рода программное обеспечение по своему функциональному назначению предназначено для предоставления удаленного доступа к зараженному компьютеру и может быть использовано злоумышленниками для шпионажа, хищения конфиденциальных и личных сведений пользователя или организации, а также для блокирования или уничтожения указанных данных[1].

Прием под названием «scareware» представляет собой введение жертвы в заблуждение посредством использования всплывающих окон на различных интернет-ресурсах, содержащих фиктивную информацию о заражении персонального компьютера жертвы вредоносным программным обеспечением. В действительности подобного рода всплывающие окна необходимы лишь для оказания психологического воздействия на жертву для дальнейшего предложения ей вредоносного программного обеспечения, направленного на хищение конфиденциальной информации пользователя под видом антивирусной программы. Таким образом, злоумышленники применяют технику внушения, пробуждая у жертвы чувство страха и подталкивая ее к установке замаскированного вредоносного программного обеспечения.

Прием «rogueattack» схож с вышеприведенным приемом «scareware» и представляет собой установку вредоносного программного обеспечения на компьютер жертвы под предлогом установки той или иной легальной и безопасной программы. После проведенной инсталляции установленная программа создает на персональном компьютере жертвы всплывающие окна и оповещения, которые рекомендуют жертве загрузить новую версию программы или иное «безопасное» программное обеспечение, которое чаще всего оказывается «троянским конем», после установки которого злоумышленники получают удаленный доступ к компьютеру жертвы или конфиденциальную информацию, хранящуюся на ее устройстве.

[1] См.: Приговор Ковровского городского суда Владимирской области от 26 октября 2023 г. по делу № 1-36/2023 // Ковровский городской суд Владимирской области : сайт. URL: https://sudact.ru/regular/doc/yKACyWLbR9Zb/?regular-txt=Trojan&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=10&regular-area=&regular-court=&regular-judge=&snippet_pos=5384#snippet (дата обращения: 19.03.2025).

Прием «baiting» схож с приемом «дорожное яблоко». В обоих случаях злоумышленник использует своего рода приманку для жертвы и ее любопытство. Отличием данных приемов друг от друга может явиться тот факт, что прием baiting применяется в пространстве сети Интернет и вредоносное программное обеспечение не записывается злоумышленниками на отдельные внешние носители информации (флеш-накопители, жесткие диски, карты памяти, компакт-диски и т. п.), а содержатся в самих ресурсах сети Интернет. При просмотре интернет-ресурсов пользователям часто попадается привлекательная реклама или ссылки на установку бесплатного программного обеспечения, которые, как правило, ведут на вредоносные сайты или побуждают жертву устанавливать зараженное программное обеспечение.

Такой прием, как «water-holling», представляет собой внедрение вредоносного программного обеспечения в интернет-ресурсы, при посещении которых внедренный в сайт скрипт автоматически перенаправляет жертву на иной сайт с вредоносным программным обеспечением или рекламой. По данным экспертов Лаборатории Касперского, при переходе на скомпрометированный сайт также может осуществляться принудительная установка вредоносного программного обеспечения на персональный компьютер пользователя, позволяющая злоумышленникам осуществлять шпионаж и похищать информацию с компьютера жертвы[1]. Чаще всего вредоносное программное обеспечение на скомпрометированных сайтах монтируется в JavaScript или HTML-коде сайта. В основном злоумышленники используют данный прием в отношении различных тематических форумов, слабозащищенных сайтов, а также сайтов органов государственной власти и органов местного самоуправления.

Анализируя приемы социальной инженерии, совершаемые с использованием телефонных и иных переговоров с жертвой, стоит отметить схожесть приемов вишинга, смишинга и претекстинга.

Прием вишинга представляет собой телефонные переговоры злоумышленника и жертвы, в ходе которых первый выманивает у собеседника конфиденциальные сведения, в том числе о банковском счете. Так, в ходе телефонного разговора злоумышленник может представиться сотрудником оператора сотовой связи, банка или даже правоохранительных органов и под видом предложения разного рода рекламы, выяснения тех или иных обстоятельств, которые обыгрывает злоумышленник, постепенно выманивать у жертвы нужную ему информацию. Смишинг представляет собой аналогичные действия злоумышленника, с той лишь разницей, что они осуществляются не посредством телефонных переговоров, а путем обмена текстовыми сообщениями. Претекстинг представляет собой наиболее продуманный в плане подготовки и реализации прием, совершаемый злоумышленниками как при помощи телефонных переговоров, так и посредством общения с жертвой с использованием текстовых сообщений, с той лишь разницей, что в данном случае злоумышленник руководствуется заранее подготовленным текстом (сценарием) и планом действий. При использовании приема претекстинга злоумышленники часто действуют не в одиночку, а организованной преступной группой. Для претекстинга характерен масштабный подготовительный этап, в ходе которого злоумышленники осуществляют поиск помещения, где будет располагаться так называемый кол-центр, приискивают оборудование, при помощи которого будут вестись переговоры с потенциальными жертвами, абонентские номера, банковские карты, оформленные

[1] Holly Water APT: опасная вода // Kaspersky daily. Блог Касперского : сайт. URL: https://www.kaspersky.ru/blog/holy-water-apt/27912 (дата обращения: 20.03.2025).

на третьих лиц (дропов), а также необходимое программное обеспечение. Из открытых источников собирается информация о личности предполагаемых жертв, прорабатывается сценарий, в соответствии с которым злоумышленники будут вести диалог со своими жертвами. Нельзя не согласиться с Е. В. Зотиной в том, что претекстинг требует от преступника тщательной подготовки перед контактом со своей жертвой. Ему необходимы сведения о ее базовых персональных данных (имени, фамилии, отчестве). В некоторых случаях также необходима информация о личном окружении, месте работы или увлечениях. Указанную информацию не составляет труда получить в открытых источниках сети Интернет, особенно если потенциальная жертва активно ведет социальные сети и делится с окружающими в сети подробностями о личной жизни [6].

Именно претекстинг в настоящее время представляет наиболее серьезную угрозу для общества. Преступниками разрабатываются все более опасные сценарии действий. Кроме того, в современных условиях мотив и цель преступников могут не ограничиваться лишь завладением денежными средствами жертвы, а посягать и на интересы общества и государства в целом. В текущих геополитических реалиях и условиях проведения специальной военной операции злоумышленники разрабатывают сценарии, в ходе которых им удается совершать террористические акты и диверсии руками обманутых ими людей.

Один из наиболее актуальных сценариев претекстинга можно рассмотреть на примере уголовного дела, находившегося в производстве Следственного управления Следственного комитета Российской Федерации по Калужской области. Из материалов уголовного дела следует, что в один из дней июля 2024 года на мобильный телефон П. поступил телефонный звонок. Звонящий представился сотрудником одного из крупных операторов сотовой связи. В ходе телефонного разговора звонящий сообщил П. об окончании срока действия договора на предоставление услуг сотовой связи и убедил его в необходимости продления указанного договора. Затем злоумышленник предложил П. авторизоваться на странице портала «Госуслуги», для чего пришлет ему в смс-сообщении специальный код, который П. должен будет сообщить злоумышленнику. Поступивший в смс-сообщений код являлся кодом двухфакторной аутентификации, необходимым злоумышленникам для входа на страницу портала «Госуслуги» жертвы. П., будучи убежденным в том, что действительно ведет диалог с представителем компании сотовой связи, сообщил злоумышленнику присланный ему код, однако уже после того, как поддался манипуляциям, осознал, что стал жертвой мошенника и прекратил телефонный разговор. Спустя несколько минут после этого П. в мессенджере Ватсап от неизвестного пользователя, представившегося сотрудником технической поддержки портала «Госуслуги», пришло текстовое сообщение, в котором П. оповещали о том, что на его страницу якобы был выполнен вход с чужого устройства и в целях предотвращения мошеннических действий П. предлагалось перезвонить по абонентскому номеру, указанному в данном текстовом сообщении. Позвонив по этому номеру, П., полагая, что ему окажут помощь в защите от возможных мошеннических действий, вступил в диалог уже с другим преступником, действовавшим в составе организованной преступной группы с предыдущим лицом и представившимся П. сотрудником технической поддержки портала «Госуслуги». В ходе телефонного разговора П. пояснил «сотруднику технической поддержки», что возможно стал жертвой мошенников. После этого злоумышленник стал налаживать психологический контакт с жертвой, сообщив П. о сведениях, которые якобы были уже похищены неизвестными мошенниками, получившими доступ к его странице

пользователя портала «Госуслуги». В дальнейшем злоумышленник предпринял меры по дестабилизации эмоционального состояния П., сообщив ему, что на его имя было оформлено несколько кредитов в различных банках. Затем согласно разработанному сценарию злоумышленник предложил П. помощь в решении данной проблемы. В ходе дальнейшего диалога злоумышленник рекомендовал П. обратиться за помощью в Центральный банк Российской Федерации и сообщил, что имеет возможность прямо сейчас соединить П. с сотрудником указанного государственного органа. В итоге на связь с П. выходит другой преступник, исполняющий роль сотрудника Центрального банка Российской Федерации, который также осуществляет налаживание психологического контакта со своей жертвой путем высказывания скрытых угроз о серьезности произошедшего и сообщает об искренних намерениях «помочь» в сложившейся ситуации. В целях анонимизации своих действий преступник, представившийся сотрудником Центрального банка Российской Федерации, предлагает продолжить дальнейшее общение в мессенджере Телеграм, где и будет осуществляться вся дальнейшая работа с жертвой. В ходе общения злоумышленник использует специализированную терминологию, а также различные формализованные процедуры, обусловленные обыгрываемым сценарием. Так, злоумышленник в целях продолжения налаживания психологического контакта с жертвой сообщает ей о том, что Центральный банк Российской Федерации не работает с физическими лицами и для оформления согласия работы с ним П. необходимо написать письменное заявление о неразглашении конфиденциальной информации и отправить фотографию заявления злоумышленнику. Цель данного действия преступника – убедить жертву в том, что единственный человек, который может ему помочь в сложившейся ситуации, – это представившийся сотрудником Центрального банка Российской Федерации злоумышленник. Таким образом, жертва намеренно лишается возможности сообщить кому-либо о произошедшем, чтобы посторонние лица не нарушили сценарий развития событий, в котором она задействована. Затем злоумышленник сообщил П., что Центральный банк Российской Федерации готов помочь в разрешении возникшей ситуации, для чего преступник под предлогом погашения задолженностей предложил П. оформить ряд кредитов в различных банках и полученные денежные средства направить по присылаемым злоумышленником банковским реквизитам. Учитывая, что к этому моменту эмоциональное состояние жертвы дестабилизировано и она полностью доверяет преступнику, П. оформил кредит на свое имя, а после получения от злоумышленника банковских реквизитов направил денежные средства преступнику. Совершая данные действия, П. полагал, что он погашает задолженности по кредиту. Взаимодействие преступника и П. продолжалось на протяжении нескольких дней. Ежедневно злоумышленник принуждал П. оформлять новые кредиты и направлять денежные средства по присылаемым преступником реквизитам. Завершающая стадия рассматриваемого сценария заключается в том, что, после того как злоумышленник выманивает у жертвы необходимую сумму денежных средств, преступник вновь выходит на связь с жертвой, утверждая, что ей заинтересовались сотрудники правоохранительных органов, и предупреждает, что через некоторое время ей поступит звонок от сотрудника правоохранительных органов. Спустя некоторое время П. поступил звонок от третьего соучастника преступления, представившегося сотрудником правоохранительных органов. Вступив в диалог с жертвой, он пояснил, что «мошенники» якобы перевели от имени П. большую сумму денежных средств в адрес «недружественной страны» и в случае, если П. не хочет, чтобы в отношении него возбудили уголовное дело, ему следует действовать по пред-

лагаемой псевдосотрудником инструкции. Напуганный и доверившийся преступникам П., который уже на протяжении нескольких дней программировался другими мошенниками, входящими в преступную схему, соглашается на условия злоумышленника. При дальнейшем общении преступник сообщил П. о том, что мошенники, которые от имени П. направили денежные средства в адрес недружественного государства, осуществляют трудовую деятельность в том или ином государственном учреждении, как правило, в военном комиссариате или правоохранительных органах. Сообщив эту информацию, злоумышленник ввел П. в заблуждение, утверждая, что для задержания мошенников и проведения обыска в здании, где они находятся, П. должен устроить провокацию, которая заключается в поджоге пиротехнического изделия внутри помещения этого здания либо метании в него бутылки с зажигательной смесью. Доверившаяся и испуганная жертва часто соглашается совершить подобного рода действия, продолжая верить в то, что ей помогают погасить кредитные обязательства или избежать мнимого уголовного преследования, не понимая, что из-за ее действий могут пострадать другие люди.

Как следует из описанной ситуации, практически в каждом случае применения претекстинга принимают участие несколько преступников, объединенных общим преступным умыслом, каждый из которых играет свою роль в соответствии с подготовленным сценарием.

Ранее также был распространен сценарий претекстинга, при котором участвовал лишь один преступник. Он звонил своей жертве по телефону, представляясь следователем. В самом начале телефонного разговора злоумышленник задавал формальный и строгий тон разговора, уведомляя жертву об аудиозаписи их переговоров, называл свое специальное звание и место службы, объяснял, что банковская карта жертвы якобы замечена в каких-то подозрительных операциях, после чего начинал «допрос» прямо по телефону, выманивая у жертвы те или иные конфиденциальные сведения, в том числе данные банковской карты для последующего хищения с нее денежных средств.

«Кви про кво» как прием социальной инженерии представляет собой оказание психологического воздействия на жертву посредством обмана или злоупотребления доверием в целях получения конфиденциальной и иной значимой для злоумышленника информации, манипулирование поведением жертвы, ее побуждение действовать в интересах злоумышленника под видом оказания ей мнимой помощи или услуги со стороны злоумышленника. В качестве примера можно привести типовую ситуацию, характерную для этого приема. Злоумышленник выясняет факт наличия у одного из сотрудников крупной финансовой организации возможности доступа к сети или интересующим злоумышленника данным, после чего связывается с ним, представляясь ему сотрудником службы безопасности или технической поддержки указанной фирмы, а затем сообщает жертве о возникшей технической ошибке в сетевой инфраструктуре компании. В дальнейшем под предлогом мнимого исправления возникшей технической ошибки преступник просит у жертвы предоставить доступ к необходимым ему сведениям. Получив доступ к сетевой инфраструктуре компании, злоумышленник внедряет в нее вредоносное программное обеспечение или совершает хищение нужной ему конфиденциальной информации.

Прием «honeytrap» широко распространен среди пользователей сайтов знакомств, а также в социальных сетях и мессенджерах. Он заключается в создании злоумышленником фейковой страницы пользователя для вступления в диалог с пользователями противоположного пола в целях получения у жертвы конфиденциальной или иной

информации либо ее побуждения к совершению действий, выгодных преступнику. В ходе общения, которое часто может обыгрываться преступником как романтическое, обольщенная жертва передает ему все больше и больше личной и конфиденциальной информации, вплоть до сведений о банковских картах, паспортных данных. Кроме того, таким способом злоумышленник может выманивать у жертв фотографические и видеоизображения личного характера. Преступник может также получить от доверчивого собеседника и удаленный доступ к его компьютеру. Завладев указанными сведениями, злоумышленник часто прибегает к шантажу жертвы, вымогая у нее денежные средства под угрозой распространения полученных конфиденциальных сведений. Интересный пример использования данного приема в настоящее время распространен в мессенджере Телеграм и социальной сети ВКонтакте, в которых функционируют сервисы для онлайн-знакомств между случайными пользователями. Злоумышленник создает страницу пользователя в указанном чате, как правило, от лица женского пола, после чего приступает к поиску потенциальных жертв, с которыми в дальнейшем осуществляет знакомство и вступает в диалог. В ходе общения преступник от лица девушки предлагает жертве встретиться и сходить в театр или кино, поясняя собеседнику, что как раз сейчас в прокат вышла захватывающая кинокартина или идет показ интересной пьесы. Доверившаяся жертва соглашается на предложение, и злоумышленник высылает ей интернет-ссылку, ведущую на сайт, предназначенный для бронирования и оплаты билетов в кино или театр, а затем просит жертву забронировать и оплатить два билета для грядущей встречи. Далее введенная в заблуждение жертва переходит на сайт, бронирует места, вводит данные банковской карты при оплате, однако вместо приобретения билетов в кино или театр отправляет свои денежные средства на банковский счет мошенникам. Этот прием часто используется в синтезе с приемом клон-фишинга, который будет разобран далее.

«Клон-фишинг» как прием социальной инженерии заключается в копировании злоумышленниками известных интернет-ресурсов или официальных электронных писем в целях введения пользователей в заблуждение и побуждения их предоставить злоумышленникам информацию конфиденциального характера. Один из наиболее любопытных случаев применения этого приема можно рассмотреть на примере уголовного дела[1], рассматривавшегося в Калужском районном суде Калужской области. Из материалов уголовного дела следует, что в 2020–2021 гг. К. создал профиль пользователя в социальной сети ВКонтакте, подписав его в качестве администратора данной социальной сети и оформив внешний вид страницы в соответствии с внешним видом сотрудника-модератора социальной сети ВКонтакте. С указанной страницы К. направлял различным пользователям заранее подготовленный им текст, содержащий информацию о том, что страница пользователя, которому он присылал сообщение, была взломана неизвестным человеком. К. предлагал пользователям в целях предотвращения утраты доступа к странице сменить пароль и прикреплял к письму ссылку для его смены. Пользователь, получивший такое сообщение, мнимо полагавший, что ему действительно пришло письмо от администрации социальной сети ВКонтакте и желающий обезопасить страницу от посторонних лиц, переходил по содержащейся в письме интернет-ссылке, чтобы сменить пароль. В итоге он попадал на интернет-страницу для смены пароля,

[1] См.: Приговор Калужского районного суда Калужской области № 1-1-104/2022 от 8 декабря 2022 г. по делу № 1-1-104/2022 // Судебные решения : сайт. URL: https://судебныерешения.рф/72823432 (дата обращения: 21.03.2025).

которая внешне копировала стиль и оформление сайта социальной сети ВКонтакте. На ней имелось окно для ввода логина и пароля. Доверившийся пользователь вводил в него данные для входа на свою страницу, после чего они попадали в руки К., который благодаря этому без всякого труда авторизовывался на пользовательских страницах жертв и выгружал с них информацию для дальнейшего поиска личных сведений. Обнаружив те или иные конфиденциальные сведения, К. вновь связывался с жертвами и шантажировал их, вымогая у них денежные средства под угрозой распространения обнаруженной им личной информации.

Подобным образом злоумышленники также часто копируют интернет-сайты с объявлениями, например, Юла или Авито, а также известные маркетплейсы: Озон, Вайлдбериз, Алиэкспресс и др. Причем преступники не только стараются скопировать дизайн сайта, но и делают его интернет-адрес крайне схожим с оригиналом. Так, оригинальный интернет-адрес сайта Вайлдбериз – www.wildberries.com, однако злоумышленники могут сделать его визуально близким к оригиналу, заняв адрес – www.wi1dberries.com, где вместо латинской буквы I стоит цифра 1. В связи с этим особое внимание стоит уделять интернет-адресу сайта, на который переходит пользователь или на котором совершаются покупки.

Подводя итог проведенному исследованию, можно сделать вывод о том, что разработка рекомендаций по противодействию приемам социальной инженерии требует комплексного подхода, включающего в себя как применение мер технического характера, так и повышение цифровой грамотности и бдительности населения.

В соответствии с проведенным исследованием целесообразно выделить следующие ключевые рекомендации: повсеместное внедрение и использование двухфакторной или многофакторной аутентификации для ключевых учетных записей, использование генератора одноразовых кодов вместо смс-сообщений; повсеместное внедрение и использование в работе специализированного программного обеспечения, включающего в себя антивирусные программы, а также менеджеры создания уникальных паролей; внедрение и использование в работе систем обнаружения и предотвращения утечек данных (DLP) для мониторинга и передачи конфиденциальной информации; проведение обучения населения, направленного на повышение цифровой грамотности, которое может заключаться в проведении мастер-классов и тренингов по распознаванию и предотвращению атак с использованием методов социальной инженерии; повышение бдительности населения посредством уведомления об актуальных угрозах в сети, разработки и внедрения четкого регламента действий в случае обнаружения атак с применением методов социальной инженерии, осуществления систематической смены паролей на ключевых учетных записях. Кроме того, следует применять некоторые меры личной предосторожности: отказаться от загрузки на рабочее или личное устройство непроверенного программного обеспечения или программного обеспечения из ненадежных источников, в том числе по просьбе малознакомых лиц; не подключать к рабочему или личному устройству неизвестные накопители информации; отказаться от ведения телефонных переговоров при обсуждении с неизвестными лицами вопросов финансового плана.

Указанные рекомендации могут способствовать формированию комплексных мер защиты от рассмотренных приемов социальной инженерии и снизить риск успешных атак со стороны злоумышленников.

**Список источников**

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

2. 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.

3. Старостенко Н. И. Понятие и виды методов социальной инженерии, применяемых при совершении преступлений в сфере информационно-телекоммуникационных технологий // Вестник Нижегородской академии МВД России. 2023. № 1(61). С. 152–159.

4. Суворова В. В., Суворова Л. А. Совершение преступлений с использованием социальной инженерии: постановка проблемы // Теория и практика приоритетных научных исследований : сб. науч. тр. по материалам VIII Междунар. науч.-практ. конф. Смоленск : Наукосфера, 2019. С. 71–74.

5. Зотина Е. В. Криминальные детерминанты телефонного мошенничества, совершаемого с использованием приемов социальной инженерии // Вестник Казанского юридического института МВД России. 2023. Т. 8, № 1(15). С. 31–35.

6. 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.

7. Шарыпова Т. Н., Вяльцев Д. Р. Получение персональных данных с помощью социальной инженерии методом «дорожное яблоко» // Аллея науки. 2019. Т. 3, № 1(28). С. 993–996.

8. Янгаева М. О. Методы (техники) социальной инженерии, используемые при совершении преступлений в сфере компьютерной информации // Криминалистика: вчера, сегодня, завтра. 2021. Т. 18, № 2. С. 145–151.

**References**

1. Starostenko, N. I. 2024, ‘Criminalistic features of methods of committing theft using methods of social engineering and information and telecommunication technologies’, *Bulletin of the St. Petersburg University. Series Law,* vol. 15, iss. 1, pp. 152–170.

2. Starostenko, N. I. 2022, ‘Criminalistic characterization of the identity of a criminal who commits theft using social engineering methods’, *Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia,* iss. 4(58), pp. 89–95.

3. Starostenko, N. I. 2023, ‘The concept and types of social engineering methods used in the commission of crimes in the field of information and telecommunication technologies’, *Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,* iss. 1(61), pp. 152–159.

4. Suvorova, V. V. & Suvorova L. A. 2019, ‘Committing crimes using social engineering: problem statement’, in *Theory and practice of priority scientific research: collection of scientific papers based on the materials of the VIII International Scientific and Practical Conference,* pp. 71–74, Naukosphere, Smolensk.

5. Zotina, E. V. 2023, ‘Criminal determinants of telephone fraud committed using social engineering techniques’, *Kazan Law Institute of the Ministry of Internal Affairs of Russia,* vol. 8, iss. 1(15), pp. 31–35.

6. Zotina, E. V. 2022, 'Pretexting as a social engineering technique used by phone scammers: a criminological view of the problem', *Kazan Law Institute of the Ministry of Internal Affairs of Russia,* vol. 13, iss. 4(50), pp. 93–99.

7. Sharypova, T. N. & Vyaltsev, D. R. 2019, 'Obtaining personal data using the social engineering of the "road apple" methods', *Alley of Science,* vol. 3, iss. 1(28), pp. 993–996.

8. Yangaeva, M. O. 2021, 'Methods (techniques) of social engineering used in the commission of crimes in the field of computer information', *Criminology: yesterday, today, tomorrow,* vol. 18, iss. 2, pp. 145–151.

**Информация об авторе**

**В. В. Глазовский** – следователь по особо важным делам первого отдела по расследованию особо важных дел (о преступлениях прошлых лет) (Следственное управление Следственного комитета Российской Федерации по Калужской области), аспирант кафедры судебно-экспертной и оперативно-розыскной деятельности (Санкт-Петербургская академия Следственного комитета Российской Федерации).

**Information about the author**

**V. V. Glazovsky** – investigator in particularly important cases of the first department for the investigation of particularly important cases (on crimes of previous years) (Investigative Department of the Investigative Committee of the Russian Federation for the Kaluga Region), postgraduate student at the Department of Forensic Expertise and Operational Investigative Activities (St. Petersburg Academy of the Investigative Committee of the Russian Federation).

**Примечание**

Содержание статьи соответствует научной специальности 5.1.4. Уголовно-правовые науки (юридические науки).

Статья поступила в редакцию 24.05.2025; одобрена после рецензирования 02.06.2025; принята к публикации 17.06.2025.

The article was submitted 24.05.2025; approved after reviewing 02.06.2025; accepted for publication 17.06.2025.