МРНТИ 81.93.29

10.51889/2959-5894.2025.92.4.017

Ж.К. Ибраева[1*], Д.А. Ибраев[1]

[1]Сатпаев университет, г. Алматы, Казахстан
[*]*e-mail: z.ibrayeva@satbayev.university*

АНАЛИЗ УГРОЗ СОЦИАЛЬНОГО ИНЖИНИРИНГА В СОЦИАЛЬНЫХ СЕТЯХ И МЕТОДЫ БОРЬБЫ С НИМИ

Аннотация

Наблюдая растущую популярность в социальных сетях степень современной коммуникации, где предоставляется пользователям широкие возможности для обмена информацией, незримо возрастают и мер использования угроз распространения вредоносной информации, связанной с применением методов социального инжиниринга. Данная работа посвящена исследованию явления социального инжиниринга, направленного на манипулирование пользователями социальных сетей с целью извлечения конфиденциальных данных, подрыва репутации, распространения дезинформации или иного вреда. Рассматриваются релевантные основные механизмы социального инжиниринга, причины уязвимости пользователей к подобным атакам, а также потенциальные последствия для информационной безопасности. В работе предлагаются рекомендации по противодействию этому виду угроз, включая повышение цифровой грамотности, разработку защитных технологий и совершенствование регуляторных механизмов. Данное исследование актуально для специалистов в области информационной безопасности, социальных наук и всех, кто заинтересован в защите цифровой среды от манипуляций и вредоносной информации.

Ключевые слова: область информационной безопасности, цифровая грамотность, социальные сети, вредоносная информация, социальный инжиниринг, защитные технологий

Ж.К. Ибраева[1], Д.А. Ибраев[1]
1Сатпаев университеті, Алматы қ., Қазақстан

ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ ҚАУІПТЕРІН ТАЛДАУ ЖӘНЕ ОЛАРМЕН КҮРЕСУ ӘДІСТЕРІ

Аңдатпа

Әлеуметтік желілерде қазіргі заманғы коммуникацияның өсіп келе жатқан танымалдылығын бақылай отырып, пайдаланушыларға ақпарат алмасу үшін кең мүмкіндіктер берілетін жерде, әлеуметтік инженерия әдістерін қолданумен байланысты зиянды ақпарат тарату қаупінің артуы байқалады. Бұл жұмыс әлеуметтік желілерді пайдаланушыларды құпия деректерді алу, беделді түсіру, дезинформация тарату немесе басқа зиян келтіру мақсатында манипуляциялауға бағытталған әлеуметтік инженерия құбылысын зерттеуге арналған. Әлеуметтік инженерияның негізгі механизмдері, пайдаланушылардың осындай шабуылдарға осал болу себептері, сондай-ақ ақпараттық қауіпсіздікке ықтимал салдары қарастырылады. Жұмыста бұл қауіп-қатерге қарсы тұру бойынша ұсыныстар беріледі, соның ішінде цифрлық сауаттылықты арттыру, қорғаныс технологияларын әзірлеу және реттеу тетіктерін жетілдіру.

Түйін сөздер: ақпараттық қауіпсіздік саласы, Цифрлық сауаттылық, Әлеуметтік желілер, Зиянды ақпарат, Әлеуметтік инженерия, Қорғаныс технологиялары,

Zh.K. Ibrayeva[1], D.A. Ibrayev[1]
[1]Satbayev university, Almaty, Kazakhstan

ANALYSIS OF SOCIAL ENGINEERING THREATS IN SOCIAL NETWORKS AND METHODS TO COMBAT THEM

Abstract

Observing the growing popularity of social networks as a medium of modern communication, which provides users with extensive opportunities for information exchange, there is an unseen rise in the threats of

spreading malicious information associated with the use of social engineering methods. This study focuses on the phenomenon of social engineering aimed at manipulating social network users to extract confidential data, damage reputations, spread disinformation, or cause other harm. The relevant key mechanisms of social engineering, the reasons for users' vulnerability to such attacks, and the potential consequences for information security are considered. The work also offers recommendations for countering these threats, including enhancing digital literacy, developing protective technologies, and improving regulatory mechanisms. This research is relevant to specialists in the field of information security, social sciences, and anyone interested in protecting the digital environment from manipulation and malicious information.

Keywords: field of information security, digital literacy, social networks, malicious information, social engineering, protective technologies

Введение

Принимая во внимание все стороны развития социального инжиниринга, рассматриваются источники возникновения и возможные пути ее распространения. Также можно подчеркнуть быстрый рост данного вида зловредного типа атак из-за стойкой популярности используемых социальных сетей. Ввиду этого, результатом исследования служат релевантные рекомендации по противодействию распространению и возможности минимизирования их источников.

21 век – век начала цифровой жизни человечества вплотную, и социальные сети есть обязательная часть повседневной жизни современного общества. Везде социальные сети играют ключевую роль в коммуникациях, обмене информацией, организациях, сообщества и вовлечёнии в общественное мнение. По данным статистики, миллиарды людей ежедневно используют такие платформы, как Facebook, Instagram, Twitter, TikTok и другие, что составляет их необходимый элемент. Значимость социальных сетей показывает масштаб охватывания, скорость обмена и распространения данных, уровень личной заинтересованности личности, экономия времени в обычном и рабочем режиме. Однако вместе с преимуществами социальных сетей и пользой для человечества, грядут и новые угрозы, связанными с использованием их возможностей в неблаговидных целях. Из- за таких человеческих качеств, в силу характера живого существа, как безответственность (неосознанности важности своих действий и последствий своих решений), легкомысленность (отношение к важным задачам или обязанностям с недостаточной серьезностью), отсутствие внимания к деталям (допущение ошибки из-за поверхностного подхода), несобранность (неспособность организовать свою деятельность), пренебрежение обязанностями (умышленное или случайное игнорирование задач), недисциплинированность (неспособность следовать установленным правилам или графику), беспечность (уверенность, что всё «как-то само» уладится, даже без усилий), лень (отказ тратить время и силы на выполнение обязанностей качественно), непунктуальность (постоянные опоздания или несвоевременное выполнение дел), непредусмотрительность (неспособность учитывать возможные последствия своих действий) являются большими приспешниками и создают благоприятную почву для угрозы распространения частной информации.

Одним из таких угроз является социальный инжиниринг. Существует немало уязвимостей, из-за которого риск возникновения данной угрозы настолько велик, что большинство ученых выделяют социальный инжиниринг уже в отдельную область. Ими выступают повешение доверия к информации, выраженное эмоциональное воздействие, возможность включения анонимности и автоматизации действии. Социальная инженерия, по своей природе, выступает прямой атакой именно на индивида, и будет звеном спланированной компьютерной атаки. Мошеннику запросто сначала «взломать» человека и получить доступ к системе или ввести в заблуждение жертву к самостоятельным действиям запуска на компьютере вредоносных файлов, чем тратить время на поиск и эксплуатацию технических уязвимостей [1].

Цель и задачи исследования. Цель исследования выражается из малоизученных научных материалов на данный момент на процент роста угроз и атак. Ориентиром атак манипулирующего стратега становятся как обычные пользователи, так и работники

различного рода компаний и банков в зависимости от намерений. В первом случае главный побудительный фактор злоумышленника – нажива или корысть, во втором случае – получение доступа в корпоративную сеть с целью кражи данных, конкурентной разведки, нарушения системной деятельности информационных систем. По меркам информационной безопасности тщательно защищенная с использованием современных технических и аппаратных устройств, а также отрезанная от Интернета информационная система уязвима к подобным атакам, поскольку её эксплуатацией и управлением занимаются непосредственно люди, в лице работников. Значимыми задачами исследования рассматривается основные характеристики социального инжиниринга на выделения вредоносной информации в социальных сетях, типы атак, методы манипуляции и психологическое воздействие на пользователей, современные технологии для обнаружения и анализа вредоносной информации, политики и регулирование со стороны социальных платформ.

Методология исследования

Основные подходы к определению природы социального инжиниринга делаются разными учеными. Например, по словам Салахдина Ф. и Кабуч Н., социальная инженерия – это искусство влияния на людей с целью получения конфиденциальной информации, такой как пароли, адреса, банковские данные и т. д., путём использования человеческих уязвимостей. Вместо использования технологических слабостей эти атаки эксплуатируют человеческие слабости, такие как чувства, доверие и привычки, чтобы получить доступ к конфиденциальной информации или данным людей. Хотя это технически менее сложно, чем другие стратегии кибератак, социальная инженерия может причинить серьёзный ущерб жертве [2]. С ними согласятся и ученые из турецкого университета имени С. Демиреля Коюн Ариф И Жанаби Аль Ихсан, также считающие, что социальная инженерия использует распространённые аспекты человеческой психологии, такие как любопытство, вежливость, доверчивость, жадность, безрассудство, застенчивость и апатия.

На рисунке 1 в мире на 2024 год пользователей социальных сетей станет 5,037 миллиарда [3].

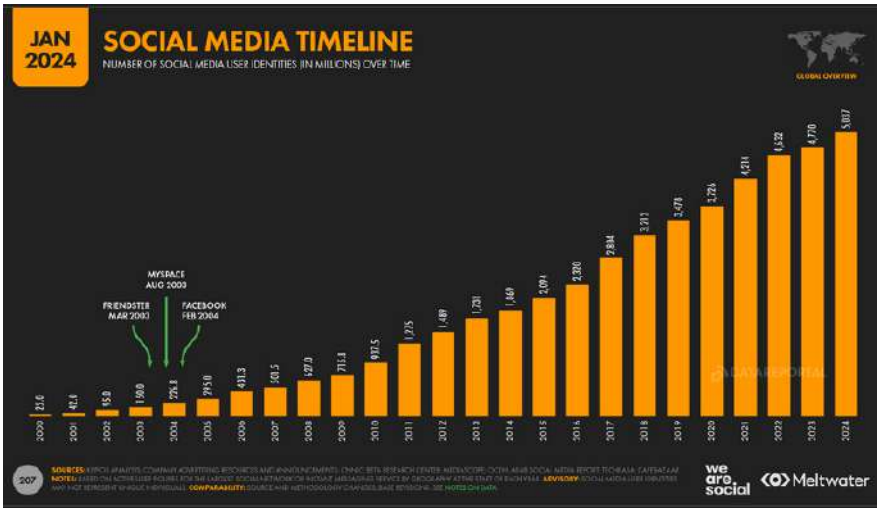

Рисунок 1. Прирост количества пользователей социальных сетей

Лидер в области кибербезопасности компания Positive Technologies ведет аналитические сводки по социальному инжинирингу, и в III квартале 2023 года, представленного на рисунке 2 из числа общего количества инцидентов именно атаки на социальные сети составили 2% (организации) и 19% (частные лица), также указала, что в основном это мошеннические действия [4].

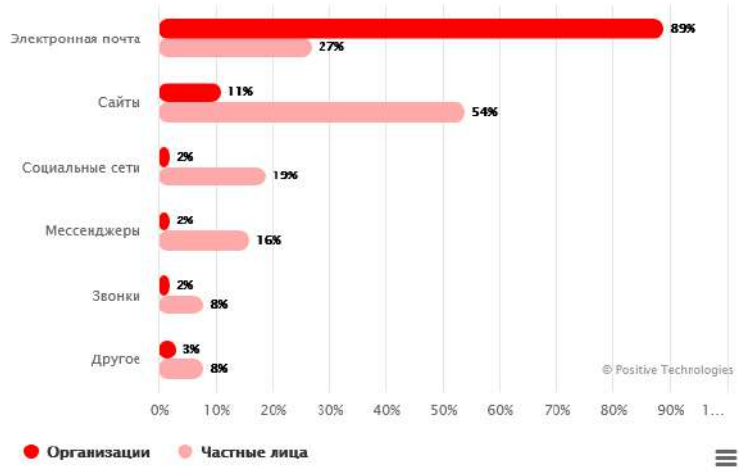

Рисунок 2. Общее количество инцидентов

Очередное доказательство того, что большинство атак совершается, именно на человека можем посмотреть на данные объектов атак как показано на рисунке 3

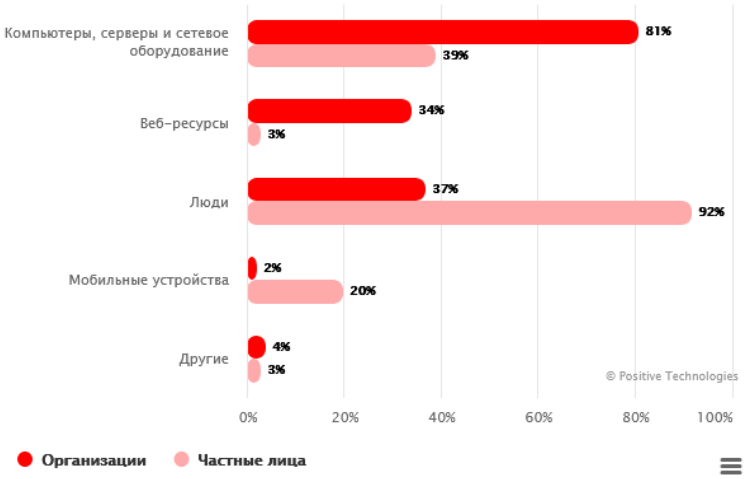

Рисунок 3. Объекты атак

Социальная инженерия наивысшей степени многогранна, что используя ее можно сделать двойную атаку, где одна завернута в другую. Данное наблюдение выделено из аналитического квартального отчета киберугроз Positive Technologies за 2024 год, где Исследователи угроз Imperva обнаружили атаку, при которой вредоносный пакет имитирует название легитимного, называемую Тайпсквоттинг, проводимую во многом в социальных сетях.

Атак и угроз социального инжиниринга довольно много, и дальнейшее их увеличение их числа напрямую зависимо от изобретательности и изощренности ума человечества, при всем при этом нам необходимо выделить те типы атак с использованием социального инжиниринга, которые непосредственно используются в социальных сетях. В – первую очередь для проведения успешного нападения проводиться исследование объекта, то есть злоумышленник изучает информацию о жертве, для одной цели – понять, как лучше всего подойти к жертве. Естественно, что анализируются профили в социальных сетях (Facebook, LinkedIn, Instagram, Twitter), собирает данные: место работы, круг общения, интересы, контакты. Завершение плана является поиск уязвимости, например, жалобы на проблемы или поиск работы.

Атака социальной инженерии, при которой злоумышленник входит в доверие к жертве, называется "претекстинг" (pretexting). Мошенники часто представляются сотрудниками различных организаций, включая банки, государственные органы и коммунальные службы, с

целью обмана граждан и получения конфиденциальной информации или денежных средств. Например, они могут выдавать себя за представителей Казпочты, сообщая о доставке заказного письма, или за сотрудников "Алматы Су", утверждая о необходимости поверки счетчиков. Под различными предлогами злоумышленники пытаются убедить жертв предоставить коды из SMS или другие личные данные. Одним из реально зафиксированных претекстинг атак в Казахстане, отмечает Национальная служба реагирования на компьютерные инциденты KZ-CERT, явилось распространение объявлений с поддельными QR-кодами в подъездах жилых домов, побуждая граждан сканировать QR-коды и присоединиться к домовым чатам в мессенджерах. Согласно отчету Калифорнийского Data Breach Investigations Report (DBIR) за 2023 год, претекстинг имеет колоссальные успехи как реализованная атака и представлена на рисунке 4 [5].

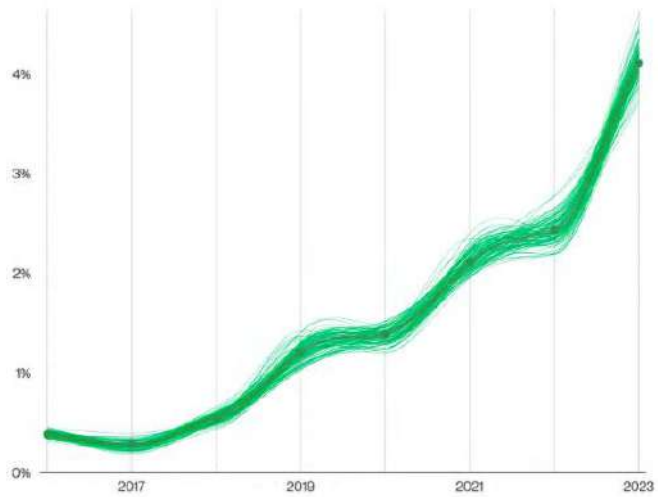

Рисунок 4. Инциденты претекстинга до 2023 года

Похожая атака, называемая фишинг (Phishing), которую по данным Государственной технической службы в 2023 году в Казахстане обнаружили 2 160 случаев. По ряду источников, от 70% до 80% фишинговых атак реализуются через сообщения, содержащие ссылки, ведущие на поддельные или заражённые сайты. Такие ссылки позволяют злоумышленникам направлять пользователей на сайты для сбора учётных данных или для автоматической загрузки вредоносного ПО. Оставшаяся часть, около 20%–30% фишинговых угроз, включает использование вредоносных вложений (например, документов, архивов или других файлов), которые при открытии могут инициировать загрузку зловредного ПО или эксплуатировать уязвимости конечных устройств. При чем в социальных сетях чаще работают только 3 вида фишинга: вишинг (vishing: использование телефонных звонков для фишинговых атак), смишинг (smishing: фишинговые атаки через SMS-сообщения), списочный фишинг (spear phishing: Целенаправленная атака на конкретного человека или организацию). За девять месяцев 2024 года зарегистрировано свыше 15,9 тыс. случаев интернет-мошенничества, что составляет около 47% от всех видов мошенничества (33 832). Общий ущерб составил порядка 26 млрд тенге. [6] По данным приложения Kaspersky Who Calls, доля пользователей в Казахстане, получавших спам-звонки, в январе–ноябре 2024 года составила 72,4%.[7] При этом более половины пользователей (52,1%) – столкнулись с мошенниками. Заметим, что почти 73% заблокировано почти 50 миллионов таких вызовов. А в сравнении с соседом Россией данные таких атак составила всего 61% за 2024 год, что показывает нам большую ориентированность мошенников именно в нашей стране.

Так, в 2020 году были зафиксированы случаи, когда пользователи получали SMS-сообщения якобы от крупных казахстанских банков, таких как Халык Банк и Казкоммерцбанк.

В этих сообщениях предупреждали о блокировке карт или счета, и предлагали перейти по ссылке для активации. Сайт, на который вели ссылки, был фальшивым, а данные карт, введенные пользователем, попадали в руки мошенников. А годом позже были распространены сообщения, якобы от Госфискальной службы Казахстана, с уведомлениями о задолженности по налогам или штрафах. В SMS предлагали перейти по ссылке для оплаты. Сайт, на который направляли жертв, имитировал официальный сайт и собирал данные для последующего использования.

Отметим разницу между ними, тем, что претекстинг фокусируется на создании индивидуального сценария и работы с конкретной жертвой, а фишинг часто массовый и менее персонализированный, обычно через поддельные письма или сообщения. В 2022 году был случай с использованием SMS-сообщений для обмана с фальшивыми уведомлениями о доставке посылок через международные компании, такие как DHL или Kazpost. В сообщениях указывали, что посылка задержана, и предлагали перейти по ссылке для уточнения адреса доставки или оплаты "дополнительных сборов". Опять же, этот сайт был фальшивым, и пользователи вводили свои данные. А уже в начале 2024 года начали поступать SMS-сообщения, которые якобы предлагали гражданам Казахстана взять кредит на выгодных условиях от крупных банков, таких как Сбербанк и Казкоммерцбанк, к тому моменту уже не существовавших. В сообщениях предлагалось пройти по ссылке для оформления кредита, где требовали ввести данные паспорта и банковской карты. Мошенники использовали эту информацию для кражи средств.

Третий вид нападения – атака Бейтинг (Baiting), это вид мошенничества, при котором злоумышленники предлагают заманчивые предложения или бесплатные товары. Например, в 2024 году в Казахстане был зафиксирован случай, когда мошенники предлагали гражданам получить водительские права без сдачи экзаменов. Они размещали объявления в социальных сетях и мессенджерах, обещая быстрое оформление документов за определенную плату. После получения денег злоумышленники прекращали связь с жертвами, а водительские права не выдавались передает агентстве по регулированию и развитию финансового рынка

И самый крупный и сложный – комбинированные атаки, использование нескольких методов одновременно.

Немаловажно рассмотреть и проанализировать исследования роста атак социальной инженерии в 2024 году, связанных с улучшением технологий, развитием методов персонализации и увеличением количества данных, доступных в открытом доступе.

По части претекстинга, в общем, по данным IBM X-Force Threat Intelligence Index – ежегодного отчета, в котором анализируются изменения в киберугрозах, выявляются тенденции и предоставляются рекомендации для защиты организаций. В выпуске отчета за 2024 год выделяются три основные тенденции, одним из которых выступает резкое увеличение случаев злоупотребления действительными учетными записями, на которые рекомендуется обратить внимание специалистам по безопасности и руководителям информационной безопасности [8]. Данные реалии вызываются увеличением персонализированных атак благодаря активному анализу профилей жертв в социальных сетях и созданию сложных сценариев обмана. Из-за причин развития технологий дипфейков и автоматизированных голосовых помощников, что позволяет злоумышленникам подделывать голос и выдавать себя за доверенных лиц. Дипфейки для атак вишинга, созданные с помощью новейших технологий генеративного ИИ, создают новый уровень обмана. Они генерируют гиперреалистичные видео, аудио и текст, которые могут ввести в заблуждение даже самых внимательных людей, приводя к многомиллионным убыткам. По данным исследователей Accenture Cyber Intelligence (ACI), злоумышленники готовы платить до 20 000 долларов за минуту высококачественного дипфейкового видео. Более того, за первый квартал 2024 года объем покупок и продаж инструментов для создания дипфейков на форумах даркнета увеличился на 223% по сравнению с первым кварталом 2023 года. К примеру, в Гонконге банк потерял 25 миллионов долларов из-за сложной дипфейковой схемы. Злоумышленники

цифровым способом воссоздали главного технологического директора компании и других сотрудников на видеозвонке, давая инструкции о переводе денег. Коллеги, не подозревая об обмане, выполнили запрос [9].

Массовое использование мобильных устройств делает SMS-сообщения эффективным инструментом для обмана для проведения смишинга, где рассылаются сообщения о "блокировке аккаунта", содержащие вредоносные ссылки для сбора данных. Symantec Internet Security Threat Report сообщает, что количество нападении смишинга выросло до 30% в 2024 году, это на 5% больше, чем в 2023 году [10].

Согласно отчёту Kaspersky Security Bulletin за 2023 год, доля целевых фишинговых атак (списочный фишинг) увеличилась с 18% в 2023 году до 25% в 2024 году. Это связано с ростом числа атак на высокопоставленных сотрудников и организации с целью получения доступа к критически важным данным. Примером такой атаки являются письма, якобы отправленные от имени генерального директора компании, с просьбой предоставить пароли или осуществить денежные переводы [11].

Согласно Cisco Annual Cybersecurity Report, злоумышленники всё чаще используют комбинированные атаки, сочетая методы фишинга, вишинга и претекстинга для повышения эффективности своих действий. Это приводит к увеличению числа атак, при которых одновременно отправляются поддельные письма и совершаются звонки, чтобы усилить доверие жертвы. Доля таких атак возросла с 10% в 2023 году до 18% в 2024 году [12]. По Harvard Cybersecurity Analysis приманки в виде заражённых USB-накопителей или QR-кодов продолжают использоваться, особенно в местах с большим количеством людей. Пример: Оставленные USB-устройства с пометкой «Конфиденциально», которые жертвы подключают к своим устройствам. Тем самым, на основании вышеизученных данных, можем привести показательную сравнительную информацию между двумя последними годами на таблице 5 и рисунке 6.

Таблица 5. Динамика атак за 2023 и 2024

	Категория	*2023 (%)*	*2024 (%)*
1	*Претекстинг*	*20*	*28*
2	*Вишинг*	*15*	*22*
3	*Смишинг*	*25*	*30*
4	*Целевой фишинг*	*18*	*25*
5	*Комбинированные атаки*	*10*	*18*
6	*Бэйтинг*	*12*	*15*

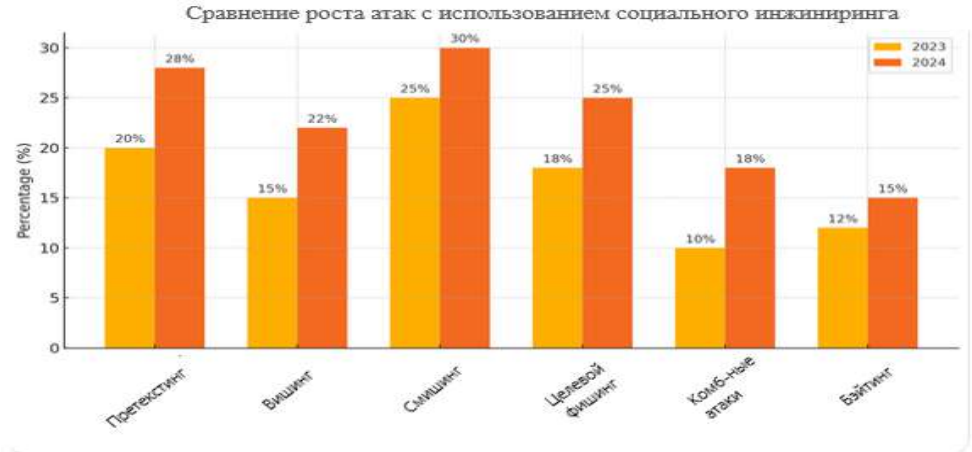

Рисунок 6. Наглядная динамика атак за 2023 и 2024

Итак, изучая все материалы по данной теме, сформулируем теоретические аспекты социального инжиниринга. Тем самым, понятие Социальный инжиниринг – это совокупность методов психологического манипулирования людьми с целью побуждения их к выполнению определённых действий или предоставлению конфиденциальной информации. Основной акцент в социальном инжиниринге делается на уязвимостях человеческого поведения, таких как доверчивость, страх, желание помочь или избежать конфликта. Выделим ключевые характеристики социального инжиниринга:

- Фокус на человеческий фактор. Злоумышленники обходят технические средства защиты, используя психологические уязвимости людей.
- Простота исполнения. Для осуществления атак часто не требуется сложных технических средств, достаточно знаний о психологии и навыков общения.
- Многообразие методов. Социальный инжиниринг включает в себя различные методы манипуляции, такие как фишинг, вишинг, смишинг, претекстинг и бейтинг.
- Использование доверия. Атаки строятся на доверии к злоумышленнику, который часто маскируется под авторитетную фигуру, коллегу или друга.
- Целевая направленность. Атаки часто нацелены на конкретных людей или группы, обладающие доступом к нужной злоумышленнику информации.

Основная задача социального инженера – «подобрать ключ» к каждому конкретному человеку и сыграть на его чувствах и эмоциях так, чтобы он забыл про осторожность и совершил необходимые злоумышленнику действия.

В методах манипуляции и психологических воздействий на пользователей социальные сети стали мощным инструментом для осуществления манипуляций и психологического воздействия, так как они предоставляют злоумышленникам доступ к большому количеству личной информации, взаимодействий и привычек пользователей.

Так в [13] автор полагает, что одной из основных криминологических детерминант телефонного мошенничества, совершаемого с использованием претекстинга, является информационная глобализация, способствующая распространению конфиденциальной информации в сети Интернет. Роль социальных сетей как платформы для реализации атак так важна, поскольку они объединяют миллиарды пользователей, создают благоприятные условия для распространения информации и обеспечивают злоумышленников инструментами для эффективного воздействия [14].

Автор рассматривает специфику методов социальной инженерии, обходящего особенности критического и аналитического мышления, используя только выявленную эмоциональную грань индивидуума [15].

Рассмотрим основные характеристики социальной инженерии:

- Социальные сети объединяют огромное количество пользователей, что делает их идеальной средой для злоумышленников. Для обоснования приведем, что в 2024 году аудитория социальных сетей насчитывала более 4,5 миллиардов человек. Такая концентрация пользователей создает большой потенциал для массовых атак, и характеризует первую характеристику - масштабную базу пользователей
- Социальные сети предоставляют злоумышленникам доступ к обширным данным пользователей, включая личные интересы, место работы, круг общения, а также контактную информацию, фото, видео, геолокацию. Тем самым подходим ко второй характерной черте, как легкий доступ к личным данным.
- Алгоритмы распространения контента социальных сетей способствуют быстрому распространению контента с высокой вовлеченностью. Важно понимать какие действия произведут зацепку внимания пользователя, то есть используются эмоционально заряженные сообщения, чтобы вызвать у пользователей желание делиться ими. К слову ложные новости, распространяются через репосты и лайки, привлекая внимание человека
- Социальные сети, как среда, имеющая несколько типов правил информационной безопасности, по признанию пользователей воспринимаются безопасной средой для общения,

что снижает их бдительность. Объясняется это легко, склонностью доверять сообщениям от "друзей" или коллег, не проверяя их подлинность. Из – за «доверия» всегда создается ложное чувство безопасности.

- Социальные сети предоставляют мощные инструменты таргетинга, которые могут быть использованы не только рекламодателями, но и злоумышленниками. Примером может служит, что полезные функции таргетинга позволяют злоумышленникам нацеливаться на определённые группы, например, сотрудников компаний или пользователей с определёнными интересами.
- Социальные сети позволяют злоумышленникам скрывать свою личность через фейковые аккаунты, что понимается как шестой характеристикой «поддержкой анонимности». Это усложняет процесс обнаружения и предотвращения атак. То есть создание поддельного профиля сотрудника отдела кадров для выманивания резюме и личных данных.

Так как социальные сети свободная площадка для рассылки всякого рода ссылок и программного обеспечения, многие пользователи переходят по ссылкам, не задумываясь об их безопасности. Принимая информацию от друга со ссылкой на якобы интересное видео, можно заразить свое устройство. Это межа распространения вредоносных ссылок и программного обеспечения.

Полезная фишка социальных сетей применение механизированных помощников ботов кроет в себе одновременно отрицательную линию, такую как возможность проводить атаки в больших масштабах с минимальными затратами. Чат-боты в социальных сетях могут быть использованы для автоматизированного вымогательства информации или распространения фишинговых ссылок. К примеру, бот отправляет сообщения от имени службы поддержки, запрашивая данные для восстановления аккаунта.

Часто социальные сети имеют баги-ошибки в своих интерфейсах программирования (API), которые могут использоваться злоумышленниками. Эти уязвимости могут дать доступ к данным пользователей или позволить совершать действия от их имени. Использование уязвимости в виде утечки данных через API может привести к сбору паролей или другой конфиденциальной информации.

Типология вредоносной информации в социальных сетях делится на несколько основных категорий в зависимости от целей и методов её создания и распространения:

Самым особенным типом выступает ложная информация (Fake News), представляемая как новость с целью ввести аудиторию в заблуждение. Примечательно, что они создаются для провокации, манипуляции эмоциями или получения выгоды, и зачастую имеют большие цели: формирование общественного мнения, дестабилизация ситуации в обществе или организации. Часто выглядят как реальные новости, что делает их более убедительными. Поддельная новость о введении новых налогов, которая провоцирует общественное недовольство, как образец.

Еще одной формой или типом рассматривается дезинформация (Disinformation) – это намеренное распространение ложной или искажённой информации для введения в заблуждение. Намерениями выступают политическое давление, финансовые выгоды, подрыв доверия к организациям или лицам. Отмечается распространением целенаправленно, часто подкрепляется манипулятивными данными, например, сфабрикованными фотографиями или видео. Пример: сообщения о якобы обострении военного конфликта, чтобы посеять панику.

Третьим типом служит Пропаганда – это информация, распространяемая для формирования определённого взгляда или поведения в интересах отдельной группы или государства. Особенностью выглядит акцент на эмоциональной манипуляции и используется в политических и идеологических целях. Пример: Сообщения, усиливающие враждебность между различными социальными или этническими группами. Цели: Контроль общественного мнения. Поддержка определённой идеологии или политики.

Разновидность в виде клеветы (Defamation) такая же ложная информация, распространяемая для дискредитации репутации человека или организации. Специфично

чаще направлена на конкретные личности или компании, и может включать ложные обвинения, слухи или фабрикованные доказательства. Пример: Публикация ложных обвинений в коррупции против политического деятеля. Замыслом представляется подрыв доверия, подготовка почвы для конкурентной борьбы. Массовое распространение ненужного или раздражающего контента является Спамом, а кликбейт – это заголовки или изображения, созданные для привлечения внимания с целью повышения трафика. Манипуляция фактами заключается в изменении контекста или акцентов фактической информации, чтобы создать ложное впечатление. Использование реальной информации, но подача в искаженном виде, вместе с этим часто применяются обрезанные цитаты, вырванные из контекста примечательно уникальны. Ложная информация, вредоносные розыгрыши (Hoaxes), распространяемая в шуточной или провокационной формы направлены на вызов массовой реакции, а именно дестабилизация, апробация социального эксперимента. Имеют короткий срок действия, но могут причинить значительный ущерб. Как способ – это сообщения о взрыве в городе, которые провоцируют панику.

Результаты исследования

В результате исследования можно ранжировать прямые риски, которые используются в социальных сетях.

Создание фейковых аккаунтов и выдача себя за другое лицо, согласно итальянским экспертам по информационной безопасности, в социальной сети Instagram составляет порядка 40%, а в Facebook насчитали около 25 тыс. таких аккаунтов, паралелльно в TikTok около 20-30 тысяч.

Риски:

- *угрозы репутации:*
  - мошенники могут приобретать аккаунты для имитации голоса бренда;
  - возможно создание фейковых представительств компании;
  - риск распространения дезинформации от имени бренда.
- *искажение метрик:*
  - накрутка ботами искажает реальные показатели эффективности – часто применяется при отчетности подрядчиками или сотрудниками;
- *риск принятия финансовых рисков:*
  - неверных маркетинговых решений.
  - потенциальные убытки от репутационного ущерба;
  - затраты на борьбу с последствиями мошенничества;
  - необходимость дополнительных инвестиций в безопасность.

В 2023 году видеоконтент стал неотъемлемой частью крупных сообществ, особенно в формате коротких видео. Этот тренд сохраняется и в 2024 году, что свидетельствует о повышенном интересе аудитории к динамичному и сенсационному контенту. К примеру, в Тульской области РФ с 2023 по 2024 год количество фейков увеличилось на 47%, а общее число просмотров фейковых новостей превысило 13 миллионов, из которых 4 миллиона – уникальные просмотры. Однако, наряду с ростом популярности сенсационного контента, увеличивается и распространение фейковых новостей. Возможные риски:

- Этические и правовые последствия: судебные иски за клевету или нарушение авторских прав.
- Психологическое воздействие: манипулировать множеством чувств пользователя, вызывать стресс, тревогу или даже панические атаки.
- Зависимость от сенсации: Постоянное потребление сенсационного контента может привести к привыканию, когда пользователи начинают искать все более экстремальные материалы, что затрудняет восприятие менее «ярких» и более нейтральных новостей.

Атаки "Лайки" или использование инструментов социальных сетей несут риски:

- Потеря конфиденциальности;

- Автоматизированные системы могут создавать фальшивые лайки и репосты;
- Мобилизация агрессивных групп.

Риски, которые несет претекстинг в социальных сетях:

- Потеря доступа к аккаунтам;
- Риск использования корпоративных аккаунтов;
- Использование карьерных амбиций и доверия к профессиональным платформам.

Роль кибергигиены и обучения пользователей. Чтобы изучить важность образования в области кибергигиены, где существуют различные "человеческие факторы", которые могут увеличивать или уменьшать вероятность стать жертвой кибератаки, взлома или утечки данных (а иногда и повторно), подчеркнем преимущества ответственного и качественного обучения в области безопасности и защиты персональных данных. Успешные методы и стратегии обучения кибергигиене включают участие ответственных государственных структур, образовательных учреждений, неправительственных организаций и всего общества [16].

Дискуссия

Кибергигиена, безусловно, важна для обеспечения кибербезопасности, но она не обязательно является ее синонимом. В то время как кибербезопасность представляет собой объективное измерение мер, принимаемых для поддержания безопасности и усиления защиты от кибератак, кибергигиена связана с знаниями и практиками интернет-безопасности, направленными на дальнейшее улучшение кибербезопасности. Выводом улучшения кибербезопасности, является необходимость улучшения киберобразования [17]. Учеными Pajaziti, A., Basholli, F. и Zhaveli, Y. приведена таблица в их статье, где можно увидеть образовательный разрыв в области кибербезопасности и необходимость обязательного обучения кибергигиене для всех, включая профессии, использующие информационные технологии в своей работе [18]. Опираясь на все изученные данные сформирован mind map по угрозам и мерам по их минимизации (рисунок 7).

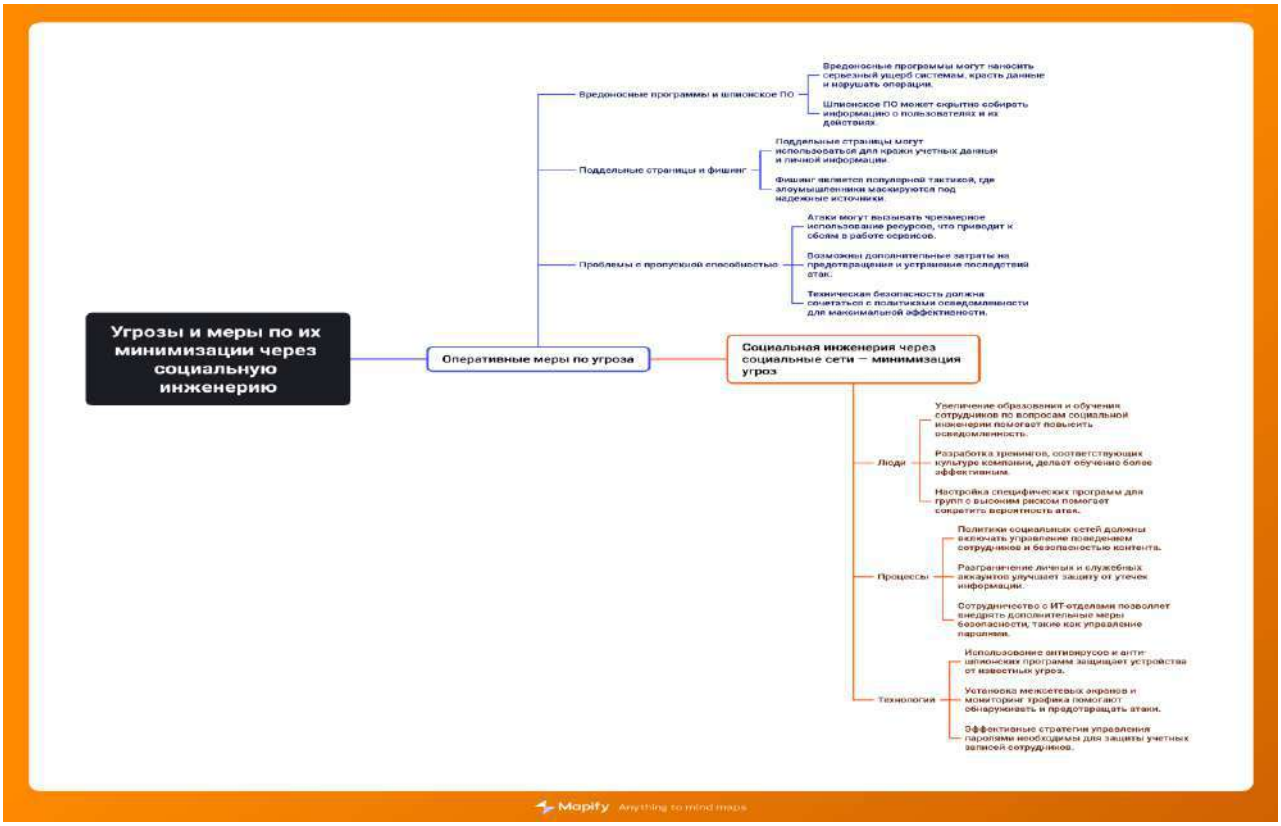

Рисунок 7. Mind map на основе изученных материалов

Заключение

Выводом данной работы является то, что основным способом защиты от атак с использованием техник социальной инженерии является повышение осведомленности пользователей. Только личная бдительность и критический подход позволит распознать угрозу социальной инженерии и признаки манипуляции пользовательскими действиями.

Если речь идет о компании, то все сотрудники должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации компании, а также о способах предотвращения утечки данных из – за лжеруководства [19]. Подтверждают вышесказанное, пришедшие к таким выводам авторы Kaouthar Chetioui, Birom Bah, Abderrahim Ouali Alami, Ayoub Bahnasse в своей статье, делая обзор на атаки социальной инженерии в социальных сетях [20]. Лучше всего это реализовать с помощью разработки четких и ясных инструкций, в которых будет прописано, какую информацию можно предоставлять другим лицам (посетителям, коллегам, в службу технической поддержки). Это также соответствует политике информационной безопасности. Следуя вышеуказанным данным, четко вырабатывается разграничение правил информационной безопасности, которые продемонстрированы на рисунке 8.

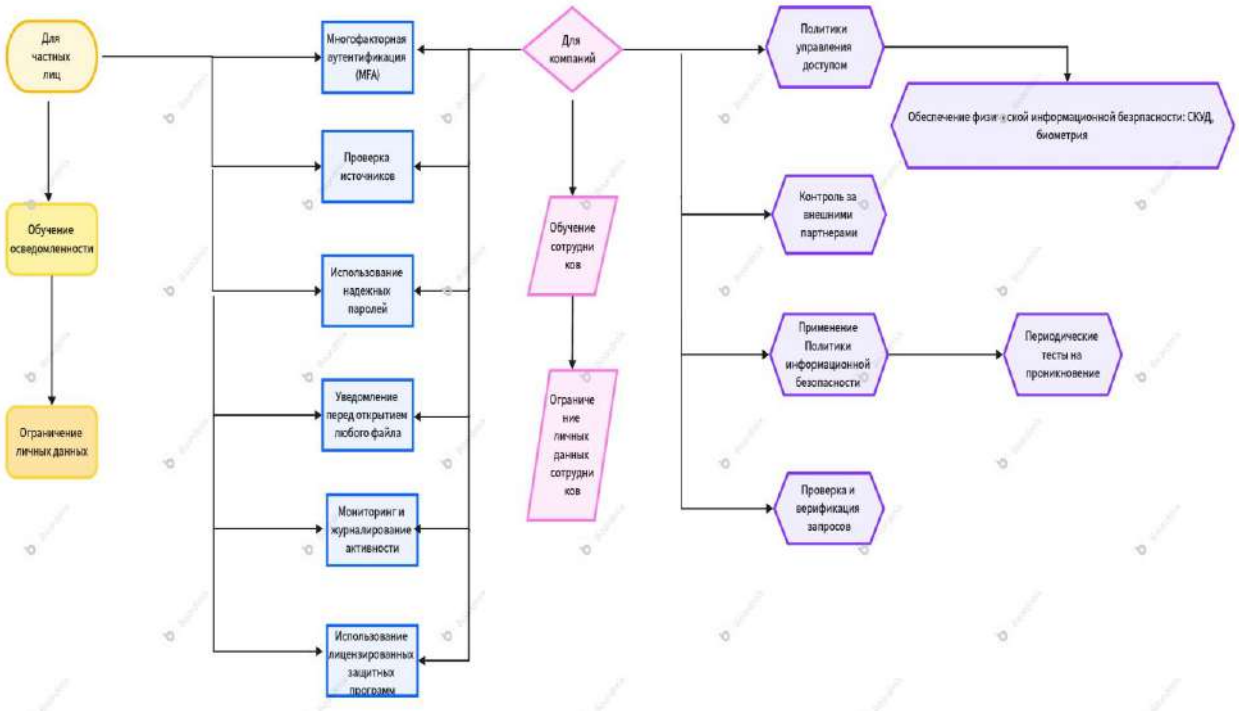

Рисунок 8. Проанализированная схема рекомендаций

Как показано на рисунке 8, эффективная защита от подобных атак требует комплексного подхода, включающего меры, как для частных лиц, так и для организаций.

Итоговым заключением для всех частных лиц в совокупности требующих соблюдение нескольких отличительных пунктов в своих действиях служит достойным воспрепятствованием вредоносным аспектам, а именно:

- увеличением осведомленности: обучение базовым принципам безопасности в интернете. Например, распознавание фишинговых писем и подозрительных звонков. Важно не раскрывать личную информацию незнакомцам;

- применением многофакторной аутентификации (MFA): включение двухфакторной аутентификации на аккаунтах, где это возможно (например, в банках, соцсетях, электронной почте). Это создаст дополнительный слой защиты, даже если злоумышленник узнает логин и пароль;

- сохранение бдительности в соцсетях: минимизация раскрытия личной информации в социальных сетях, особенно важных данных, которые могут помочь злоумышленникам создать убедительные фальшивые истории (например, даты рождения, адреса, место работы);

- контролирование источников: всегда проверяйте источники звонков, сообщений и писем. Никогда не доверяйте непроверенной информации, даже если она кажется легитимной (например, просьбы о помощи или срочные запросы);

- использование надежных паролей и их периодичное изменение: использование уникальных, сложных паролей для разных аккаунтов. Это поможет минимизировать риски, если один из аккаунтов будет скомпрометирован;

- внимательность к запросам: если кто-то неожиданно просит личную информацию или деньги, всегда уточняйте у них через независимый канал связи.

Касательно компаний, где варьируется количество физических лиц необходимо применить защиту двух уровней: защита персонального лица и защита компаний в целом с сотрудниками.

Стандартно начинается все с обучения и переобучения сотрудников. Регулярное обучение персонала по безопасности, включая тренировки по распознаванию фишинга, вишинга, смишинга и других типов атак. Важно, чтобы каждый сотрудник понимал угрозы и знал, как реагировать на них. Здесь же стоит соблюсти ограничение личных данных сотрудников. В данном направлении разрабатываются политики по минимизации распространения личной информации сотрудников. Использование минимального набора данных в корпоративных системах, а также ограничение доступа к персональным данным, которые могут быть использованы для манипуляций. Переходя к целому, устанавливаются политики управления доступом. Применение принципа наименьших привилегий: сотрудники должны иметь доступ только к тем данным и системам, которые необходимы для их работы. Это ограничит возможный ущерб от социальной инженерии. Также на разных ступенях настраивать многофакторную аутентификацию (MFA). Настройка многофакторной аутентификации для всех критичных систем, включая доступ к корпоративной сети, данным и финансовым системам. Данная работа противодействуют замыслам злоумышленникам. В рабочих средах производить проверку и верификацию запросов, как от сотрудников, так и от программного обеспечения. Установить строгие процедуры для верификации запросов на переводы средств, изменения в системах или доступах. Например, подтверждение таких запросов через несколько каналов связи.

Не обойдется и без большого пентестинга. Это проведение периодических тестов на проникновение. Автоматизированно настроенное проведение симуляций фишинговых атак и других типов социальных инжиниринговых атак, чтобы оценить уровень готовности сотрудников и проверить защитные меры.

Постоянный мониторинг и журналирование активности работы, как персонального места, так и систем в сумме. Настройка систем мониторинга для отслеживания подозрительных действий в корпоративной сети. Это может помочь быстро обнаружить попытки социального инжиниринга и предотвратить их последствия. Во избежание работы инсайдеров осуществлять контроль за внешними партнерами. А именно усиление мер безопасности при работе с внешними подрядчиками и партнерами. Важно контролировать, что их действия не ставят под угрозу безопасность компании (например, предоставление доступа к корпоративной информации).

Таким образом, противодействие угрозам социального инжиниринга возможно только при системном подходе и постоянном повышении уровня киберграмотности пользователей. Совмещение технологических и образовательных мер позволит создать надежную систему защиты, как для отдельных пользователей, так и для крупных организаций.

Список использованных источников

[1] Янгаева М.О. Социальная инженерия как способ совершения киберпреступлении// Вестник Сибирского юридического института МВД России – 2021 –№ 1 (42) – с.132 URL: https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-sposob-soversheniya-kiberprestupleniy/viewer:

[2] Salahdine F., Kaabouch N. (2019) Social Engineering Attacks: A survey] Future Internet 11,no.4:89. https://doi.org/10.3390/fi11040089

[3] Kemp S. Digital 2024: Global overview report//Datareportal [Электронный ресурс]–2024. – URL:https://datareportal.com/reports/digital-2024-global-overview-report (дата обращения 09.01.2025)

[4] Актуальные киберугрозы: III квартал 2023 года//Positive Technology [Электронный ресурс]–2023. – URL:https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/ (дата обращения 11.01.2025)

[5] Data Breach Investigations Report//Verizon [Электронный ресурс] – 2023. – URL: https://www.verizon.com/business/resources/T8f0/reports/2023-data-breach-investigations-report-dbir.pdf (датаобращения 12.01.2025)

[6]Фишинги, дипфейки и Qr – код: какие схемы распространены среди интернет – мошенников// Fingramota Online[Электронный ресурс]–2024. – URL: https://online.fingramota.kz/ru/news/view/7746 (дата обращения 12.01.2025)

[7] В 2024 году каждый второй пользователь в Казахстане столкнулся с телефонным мошенничеством//Profit [Электронный ресурс]–2024. – URL:https://profit.kz/news/68517/V-2024-godu-kazhdij-vtoroj-polzovatel-v-Kazahstane-stolknulsya-s-telefonnim-moshennichestvom (дата обращения 12.01.2025)

[8] Henderson Ch. X-Force Threat Intelligence Index 2024 reveals stolen credentials as top risk, with AI attacks on the horizon// IBM [Электронный ресурс]– 2024. – URL: https://www.ibm.com/think/x-force/2024-x-force-threat-intelligence-index (дата обращения 13.01.2025)

[9] Beyond the illusion-unmasking the real threats of deepfakes// Accenture [Электронный ресурс]–2024. – URL: https://www.accenture.com/us-en/blogs/security/beyond-illusion-unmasking-real-threats-deepfakes (датаобращения 13.01.2025)

[10] ISTR 24: Symantec's Annual Threat Report Reveals More Ambitious and Destructive Attacks [Электронный ресурс]–2024. – URL:https://www.security.com/threat-intelligence/istr-24-cyber-security-threat-landscape (дата обращения 13.01.2025)

[11] Атаки через веб-ресурсы//Kaspersky Security Bulletin [Электронный ресурс]–2023. – URL:https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/11/28132907/KSB_statistics_2023_ru.pdf (дата обращения 15.01.2025)

[12] Cisco Cyber Threat Trends Report // Cisco [Электронный ресурс] – 2024. – URL: https://www.cisco.com/c/en/us/products/security/cyber-threat-trends-report.html?utm_medium=web-referral&utm_source=cisco&utm_campaign=CSA-FY24-Q4-Content-Ebook-Cyber-Threat-Trends-Report&utm_term=pgm (дата обращения 16.01.2025)

[13] Зотина Е.В. Криминологические детерминанты телефонного мошенничества, совершаемого с использованием приемов социальной инженерии // Ученые записки Казанского юридического института МВД России. 2023. Т. 8. № 1 (15). С. 31 – 35. https://cyberleninka.ru/article/n/kriminologicheskie-determinanty-telefonnogo-moshennichestva-sovershaemogo-s-ispolzovaniem-priemov-sotsialnoy-inzhenerii/viewer

[14] Дьяков Н.В. Применение методов социальной инженерии в социальных сетях// Общество. 2020. № 2(17). URL:https://www.elibrary.ru/item.asp?id=44033034

[15] Старостенко Н.И. Социальная инженерия как объект криминалистического изучения // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 1. С. 109-114. https://doi:10.37973/KUI.2021.45.18.017

[16] Basholli, A., Mema, B., Basholli, F., Hyka, D., &Salillari, D.(2023). The role of education in cyber hygiene.// Advanced engineering Days, 7, 178-181 URL: https://www.researchgate.net/publication/373077128_The_role_of_education_in_cyber_hygiene

[17] Prummer J., T. van Steen, B.van den Berg. A Systematic Review of cybersecurity training methods// Computers and Security 2024, Vol.136. https://doi.org/10.1016/j.cose.2023.103585

[18] Pajaziti, A., Basholli, F., &Zhaveli, Y.(2023) Identification and classification of fruits through robotic system by using artificial intelligence// Engineering Applications, 2(2), 154-163. URL:

https://www.researchgate.net/publication/373140125_Identification_and_classification_of_fruits_through_robotic_system_by_using_artificial_intelligence

[19] Головин А.Ю., Головина Е.В. Социальная инженерия в механизме преступной деятельности в сфере информационно телекоммуникационных технологий. //Известия ТулГУ. Экономическиеюридическиенауки. 2021. №2 с. 3-13 https://doi:10.24412/2071-6184-2021-2-3-13

[20] Chetioui K., Bah B., Alami A., Bahnasse A. Overview of Social Engineering Attacks on Social Networks //Procedia Computer Science, Vol.198, 2022, p.656–661. https://doi:10.1016/j.procs.2021.12.302

References

[1] Yangayeva M.O. (2021) Social'nayainzheneriyakaksposobsoversheniyakiberprestuplenii [Social engineering as a way of committing cubercrimes]. VestnikSibirskogojuridicheskogoinstituta MVD Rossii. № 1 (42), 132. URL https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-sposob-sovershen iya-kiberprestupleniy/viewer (In Russian)

[2] Salahdine F., Kaabouch N. (2019) Social Engineering Attacks: A survey// Future Internet 11, no.4:89. https://doi.org/10.3390/fi11040089 (In English)

[3] Kemp S. Digital 2024: Global overview report//Datareportal [Electronic resourse] (2024) URL:https://datareportal.com/reports/digital-2024-global-overview-report (Accessed: 09.01.2025)

[4] Aktual'nyekiberugrozy: III kvartal 2023 goda [Current Cyber Threats: Q3 2023]. Positive Technology [Electronic resourse]–2023. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/ (Accessed: 11.01.2025) (In Russian)

[5] Data Breach Investigations Report//Verizon [Electronic resourse] 2023. URL:https://www.verizon.com/business/resources/T8f0/reports/2023-data-breach-investigations-report-dbir.pdf (Accessed: 12.01.2025)

[6] Fishingi, dipfejkiiQr – kod: kakieshemyrasprastranenysredi internet – moshennikov [Phishing, deepfakes and Qr-codes: what schemes are common among online scammers]. Fingramota Online [Electronic resourse]. 2024. URL:https://online.fingramota.kz/ru/news/view/7746 (Accessed: 12.01.2025) (In Russian)

[7] V 2024 godukazhdyjvtorojpol'zovatel' v Kazahstanestolknulsja s telefonnymmoshennichestvom//Profit [Electronic resourse]. 2024. URL: https://profit.kz/news/68517/V-2024-godu-kazhdij-vtoroj-polzovatel-v-Kazahstane-stolknulsya-s-telefonnim-moshennichestvom (Accessed: 12.01.2025) (In Russian)

[8] Henderson Ch. X-Force Threat Intelligence Index 2024 reveals stolen credentials as top risk, with AI attacks on the horizon// IBM [Electronic resourse]. 2024. URL: https://www.ibm.com/think/x-force/2024-x-force-threat-intelligence-index (Accessed: 13.01.2025)

[9] Beyond the illusion-unmasking the real threats of deepfakes// Accenture [Electronic resourse]–2024. URL: https://www.accenture.com/us-en/blogs/security/beyond-illusion-unmasking-real-threats-deepfakes (Accessed: 13.01.2025)

[10] ISTR 24: Symantec's Annual Threat Report Reveals More Ambitious and Destructive Attacks [Electronic resourse]. 2024. URL:https://www.security.com/threat-intelligence/istr-24-cyber-security-threat-landscape (Accessed: 13.01.2025)

[11] Atakicherezveb-resursy [Attacks via web resources]. Kaspersky Security Bulletin [Electronic resourse]. 2023. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/11/28132907/KSB_statistics_2023_ru.pdf (Accessed: 15.01.2025) (In Russian)

[12] Cisco Cyber Threat Trends Report. Cisco [Electronic resourse]. 2024. URL: https://www.cisco.com/c/en/us/products/security/cyber-threat-trends-report.html?utm_medium=web-referral&utm_source=cisco&utm_campaign=CSA-FY24-Q4-Content-Ebook-Cyber-Threat-Trends-Report&utm_term=pgm (Accessed: 16.01.2025)

[13] Zotina E.V. (2023) Kriminologicheskie determinant telefonnogo moshennichestva, sovershaemogo s ispol'zovaniempriemovsocial'nojinzhenerii [Criminological determinants of telephone fraud committed with the use social engineering]. Uchenyezapiski Kazanskogo juridicheskogo institute MVD Rossii. V. 8. No 1 (15). 31 – 35. https://doi:10.24412/2587-0661-2023-1-31-35 (In Russian)

[14] D'jakov N.V. (2020) Primenenie metodov social'noj inzhenerii v social'nyhsetiah [Application of social engineering methods in social networks]. Obshestvo. № 2(17). URL:https://www.elibrary.ru/item.asp?id=44033034 (In Russian)

[15] Starostenko N.I. (2021) Social'naja inzhenerija kak ob'ekt kriminalisticheskogo izuchenija [Social engineering as an object of forensic study]. Vestnik Kazanskogo juridicheskogo institute MVD Rossii. V. 12, No 1. 109-114. (In Russian) https://doi:10.37973/KUI.2021.45.18.017 .

[16] Basholli, A., Mema, B., Basholli, F., Hyka, D., &Salillari, D. (2023). The role of education in cyber hygiene. Advanced engineering Days, 7, 178-181. https://www.researchgate.net/publication/373077128_The_role_of_education_in_cyber_hygiene (In English)

[17] Prummer J., T. van Steen, B.van den Berg. (2024) A Systematic Review of cybersecurity training methods// Computers and Security 2024, Vol.136. (In English) https://doi.org/10.1016/j.cose.2023.103585

[18] Pajaziti, A., Basholli, F., &Zhaveli, Y. (2023). Identification and classification of fruits through robotic system by using artificial intelligence. Engineering Applications, 2(2), 154-163. URL: https://www.researchgate.net/publication/373140125_Identification_and_classification_of_fruits_through_robotic_system_by_using_artificial_intelligence (In English)

[19] Golovin A. Ju., Golovina E.V. (2021) Social'naja inzhenerija v mehanizme prestupnoj dejatel'nosti v sfere informacionno - telekommunikacionnyh tehnologii [Social engineering in the mechanism of criminal activity in the field of information and telecommunications technologies]// Izvestija TulGU. Jekonomicheskiei juridicheskie nauki, no. 2, 3-13 (In Russian) https://doi:10.24412/2071-6184-2021-2-3-13

[20] Chetioui K., Bah B., Alami A., Bahnasse A. (2022) Overview of Social Engineering Attacks on Social Networks//Procedia Computer Science, Vol.198, 656–661. (In English) https://doi:10.1016/j.procs.2021.12.302