Социоинженерные атаки: факторы успеха и способы их нейтрализации

Т. В. Тулупьева, М. В. Абрамов, А. А. Азаров

***Аннотация*—Данная статья направлена на изучение феномена социоинженерных атак и выявление ключевых факторов, обеспечивающих их успешность, а также определение путей повышения эффективности защиты от них. Проведенный обзор существующих научных трудов демонстрирует, что социоинженерные атаки отличаются высоким уровнем адаптивности и широким спектром применяемых методов манипуляции, что делает традиционные меры борьбы недостаточными. Особое внимание уделяется психологии злоумышленников, использующих понимание человеческой психологии и эксплуатации уязвимостей сознания и поведения людей. Однако, основной фокус делается на уязвимости пользователей, подчеркивая, что человеческий фактор является ключевой мишенью, а технические средства играют второстепенную роль. Важным результатом исследования является выделение направлений дальнейшего научного поиска и практической деятельности. Необходимо развивать интегрированные подходы к защите, сочетать технические меры с повышением осведомленности пользователей и внедрением кибербезопасности. Применение специальных аналитических систем, построенных на технологиях искусственного интеллекта, предлагается как перспективный инструмент раннего предупреждения и нейтрализации угроз. Обобщая выводы, авторы делают акцент на важности интеграции дисциплинарных знаний, сочетания усилий специалистов разного профиля для выработки комплексной стратегии защиты. Рекомендуется усилить подготовку кадров в области информационной безопасности, формировать устойчивые компетенции у сотрудников и включить элементы кибербезопасности в школьные учебные планы. Статья формирует основу для будущих разработок и внедрения инноваций в практику информационной безопасности, делая упор на многогранность и мультидисциплинарность решаемых задач.**

***Ключевые слова*—Социоинженерная атака, уязвимость пользователя, злоумышленник, кибератака, информационная система**

I. Введение

Информационные системы в современной организации постоянно находятся под угрозой различных типов кибератак, среди которых значительный интерес вызывают социоинженерные атаки. Данный вид атак направлен исключительно на эксплуатацию человеческого фактора посредством методик манипулирования сознанием и поведением индивидов с целью получения несанкционированного доступа к охраняемым ресурсам [1]. Эффективность таких атак обусловливается психологическими механизмами восприятия и принятия решений пользователями, подверженными воздействию социальных стимулов и обманных стратегий.

Исследование факторов, способствующих успешности социоинженерных атак, обусловлено рядом существенных тенденций в области информационной среды. Прежде всего, несмотря на существенное повышение уровня информированности общества о рисках киберпреступности, наблюдается устойчивый рост числа успешно реализуемых атак. Согласно последним отчетам международных исследовательских центров, ежегодное увеличение количества социоинженерных инцидентов составляет около 20–25%, причем каждый пятый случай становится причиной серьезных последствий для пострадавших организаций [2]. Во-вторых, большинство таких атак осуществляется путем эксплуатации доверительных отношений между сотрудниками компаний и их клиентами, либо поставщиками. Именно здесь проявляется ключевое отличие социоинженерных атак от традиционных техник взлома систем — использование человеческого фактора делает защиту значительно сложнее и требует особого подхода к обучению персонала и разработке мер превентивной безопасности. Киберпреступность некоторыми авторами рассматривается как социальная проблема, и чрезмерная ориентация на техническую составляющую в изучении киберпреступности ведёт к игнорированию ее социальных корней, что существенно снижает эффективность противодействия данному виду преступности [3], [4].

Кроме того, высокий процент успешного проникновения злоумышленников в корпоративные сети свидетельствует о недостаточной подготовке сотрудников к таким видам угроз. Компания Proofpoint, специализирующаяся на обеспечении информационной безопасности, провела в 2023 году комплексное исследование, в рамках которого было опрошено 1600 руководителей служб информационной безопасности из разных государств [5]. Результаты опроса показали, что 70% респондентов выражают серьёзную озабоченность потенциальными массированными кибератаками, запланированными против их организаций в 2024 году,

Статья получена _10_ октября 2025.

Т. В. Тулупьева, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, РАНХиГС (tulupeva-tv@ranepa.ru)

М. В. Абрамов, Санкт-Петербургский федеральный исследовательский центр Российской академии наук, СПб ФИЦ РАН (mva@dscs.pro)

А. А. Азаров, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, РАНХиГС (azarov-aa@ranepa.ru)

ввиду неуверенности в способности эффективно им противостоять. Опрос выявил также, что подавляющее большинство — 74% опрошенных специалистов — называют главной уязвимостью собственных организаций недостаточно квалифицированный персонал, обладающий недостаточными компетенциями в области кибербезопасности и цифровой грамотности. Этот вывод подчёркивает важность углубленного анализа ключевых факторов, способствующих успеху подобного рода нарушений информационной безопасности, а также поиска способов снижения значимости указанных факторов.

Современная информационная среда отличается стремительным технологическим прогрессом и нарастающей зависимостью бизнеса и повседневных процессов жизнедеятельности от информационно-коммуникационных сетей. Вместе с этим растет и угроза киберпреступности, особенно опасная форма которой представлена социоинженерными атаками. Такие нападения основаны на манипуляциях человеческим фактором и представляют значительную угрозу для информационной безопасности организаций и частных лиц. Особенностью социоинженерных атак является высокая степень вероятности их успешной реализации, поскольку они эксплуатируют социальные и когнитивные механизмы доверия, создавая условия для обхода стандартных мер технической защиты. Несмотря на широкое распространение средств предотвращения киберинцидентов, статистика показывает тревожный рост числа успешных атак такого типа, развитие кибератак большей сложности и большего масштаба [6]. Из-за многообразия форм проявления кибератак, вызванных процессами цифровизации и сетевизации общества, значительного роста их сложности и вариативности узкодисциплинарные концепции оказываются недостаточными для анализа новых явлений [7], что требует разработки междисциплинарного подхода, объединяющего знания из психологии, информатики, девиантологии, криминологии, социологии, права, семиотики, медиаисследований и математики [8].

Так, согласно последнему официальному отчету МВД России за первую половину 2025 года более трети преступлений совершается с использованием информационно-коммуникативных технологий, 38,5% в январе – июне 2024 года до 39,5% в январе – июне 2025 года [9]. Среди зафиксированных случаев выделяются случаи фишинга, вишинга и претекстинга — приемов, основанных на злоупотреблении человеческой невнимательностью и доверием.

Анализируя статистику и учитывая последствия социоинженерных атак, мы можем утверждать, что понимание их специфики и факторов успешности приобретает особую значимость для разработки эффективной стратегии защиты. Учитывая тенденции последнего десятилетия, проблема преодоления человеческих слабостей в сфере информационной безопасности выходит на первый план. Глубокое понимание механизмов криминальных действий и особенностей реагирования пользователей позволит специалистам разрабатывать высокоэффективные средства защиты, направленные на снижение ущерба от аналогичного рода происшествий.

Существуют различные подходы к обеспечению защиты пользователей, которые можно разделить на:

1. Информационные — когда пользователя пытаются научить быть внимательным, информируют о видах социоинженерных атак и наиболее распространенных способах их реализации в текущий момент времени;

2. Ограничительные — когда используются программно-технические инструменты для блокирования действия пользователей, имеющих риск скомпрометировать систему, ограничения прав доступа;

3. Провокационные — когда пользователь становится целью инсценированной социоинженерной атаки, проводимой специальной организацией или профессионалами по заданию лиц, принимающих решения в компании.

4. Превентивные — когда строится и мониторится профиль уязвимостей пользователя, в котором обновляются оценки выраженности уязвимостей.

Исследование ключевых характеристик социоинженерных атак и установление закономерностей, повышающих вероятность их успешного осуществления, открывает возможность существенного сокращения риска потерь для коммерческих предприятий и государственных учреждений, обеспечивая надежную охрану конфиденциальных сведений и предотвращение значительных экономических убытков вследствие подобных инцидентов. Следовательно, создание научно-обоснованной модели оценки угроз и внедрение действенных контрмер обладает важнейшим прикладным значением для укрепления общего уровня информационной безопасности современного общества.

Осуществляя комплексный анализ факторов, определяющих успешность социоинженерных атак, исследователи и практикующие эксперты ставят цель выявления недостатков действующих подходов к обеспечению информационной безопасности и разработки инновационных инструментов противостояния указанным угрозам. Таким образом, изучение данной проблемы способствует укреплению цифрового суверенитета государства и защите прав граждан в условиях растущих угроз информационной эпохи.

II. СОЦИОИНЖЕНЕРНЫЕ АТАКИ

Под социоинженерной атакой понимается система целенаправленных действий злоумышленника против отдельного лица или группы лиц, направленная на достижение конкретного результата, преимущественно связанного с нарушением информационной безопасности (получение несанкционированного доступа к данным, их передачу третьим лицам и проч.) [10]. Данная форма воздействия представляет собой разновидность актов социального влияния. Согласно обобщенному определению, социальное влияние предполагает изменение эмоциональной, познавательной или поведенческой сферы индивида с

целью инициирования изменений в указанных областях [11]. Применительно к социоинженерным атакам конечной целью становится модификация именно поведенческих реакций жертвы, выражающаяся в совершении ею действий, приводящих к раскрытию или утечке данных, тогда как трансформации эмоциональной и когнитивной сфер выступают вспомогательными этапами подготовки основной атаки.

Авторами к настоящему моменту разработана классификация социоинженерных атак [12] и интегральная модель социального влияния [11]. Предложенная классификация видов социоинженерных атак основана на этапах их реализации. Выделяются четыре основных этапа:

Сбор информации: включает претекстинг (создание легенды) либо рассылку без предварительного сбора информации.

Установление контакта: осуществляется посредством электронных писем (мейл-фишинг), мессенджеров (мессенджерный фишинг), телефонных звонков (вишинг), SMS-сообщений (смэшинг), социальных сетей и фальшивых веб-сайтов.

Эксплуатация доверительных отношений: разделяется на атаки поощрения (обещания выгод) и атаки угроз (шантаж, запугивание).

Исполнение атаки: заключается в действиях жертвы, приводящих к утечке данных, установке вредоносного ПО, ограничении санкционированного доступа к данным или передаче конфиденциальной информации.

Предложенная классификация охватывает широкий спектр возможных способов социальной инженерии и служит основой для систематизации рисков и мер защиты информационных ресурсов организаций и пользователей.

Модель социального влияния служит основой для описания социоинженерной атаки, в которой злоумышленник выступает в роли агента влияния, а пользователь информационной системы или держатель нужной информации, с которым можно вступить в контакт посредством технических средств, — в роли реципиента. Чем больше у злоумышленника во владении доступных ресурсов (которые входят в модель самого злоумышленника) [13], тем успешнее окажется социоинженерная атака. В модели злоумышленника можно выделить ресурсную составляющую, которая включает в себя возможность вознаграждать и наказывать в широком смысле и наличие различных материально-технических средств, компетентностную составляющую, в том числе умение выбрать правильный вид атакующего воздействия и знания об особенностях объекта влияния (потребности, психологические особенности, доступ к информационным системам). В модели реципиента можно выделить профиль уязвимостей [1], в основе которого лежит уровень выраженности его психологических, социальных особенностей и психические состояния, которые могут выступать фоном для усиления той или иной уязвимости. При совершении социального воздействия злоумышленник затрагивает психические состояния в первую очередь, поскольку, они связаны с аффективной сферой личности. При правильном подборе способов влияния и технических средств для контакта с жертвой злоумышленник с большей вероятностью достигает своей цели – вынудить жертву совершить действие, которое предоставит злоумышленнику доступ к желаемой информации или активу.

III. РЕСУРСЫ ЗЛОУМЫШЛЕННИКА

Оружием злоумышленника, позволяющим манипулировать жертвой и заставить ее подчиняться, является обмен сообщениями как письменными, так и устными. Чтобы достичь результата, злоумышленник должен поддерживать восприятие риска от общения со злоумышленником жертвой или реципиентом на низком уровне, демонстрируя качества, связанные с доверием, и обращаясь к жертве с сообщением или каким-то предложением. Кроме того, в противовес этому выигрышной стратегией злоумышленника является убеждение жертвы, что без общения с ним и без совершения определенных действий жертва рискует больше и потеряет какие-то значимые ресурсы и блага. Примером такой атаки являются звонки мошенников из, якобы, службы безопасности банка или отделения полиции с требованием перевести деньги на «безопасные» счета, чтобы сохранить их. Доверие — это представление жертвы о том, что злоумышленник выполнит данное предложение или обещание. Доверие повышает уверенность и снижает восприятие риска. Авторитет злоумышленника характеризуется следующими атрибутами: общность и репутация, которые создают у жертвы ощущение надежности. Общность — это воспринимаемая точка соприкосновения между жертвой и злоумышленником. Установив общность, злоумышленник может получить доверие, оказываемое членам группы. Общность может быть установлена путем предоставления деталей, которые известны только членам группы (контекстуализация), демонстрации знакомства с жертвой (персонализация) или разделения общих убеждений. Общность можно легко установить в Интернете, поскольку злоумышленник может использовать информацию в социальных сетях и на веб-сайтах, чтобы найти общий язык с жертвой. Используя такого рода информацию, злоумышленник может выдать себя за члена сообщества или знакомого на интернет-форумах или в группах в социальных сетях.

Репутация — это свойство, описывающее оценку другими людей о человеке или источнике. Репутация часто экстраполируется на основе таких характеристик, как партнеры (или социальные сети) и принадлежность к учреждениям.

Репутация способствует сотрудничеству, что объясняет, почему атаки социальной инженерии часто используют как социальные сети, так и принадлежность к авторитетным учреждениям. Например, злоумышленник может выдать себя за представителя власти (правительственных учреждений, департамент министерства или правоохранительные органы) или подразумевать общие связи в социальных сетях с

жертвой, чтобы добиться сотрудничества.

Социоинженерные атаки в киберпространстве по своей механике похожи на социальное воздействие в реальном мире, но наблюдается ряд отличий. Интернет пространство предоставляет злоумышленнику больше возможностей для персонализации атак, поскольку, пользователи представляют о себе много информации в открытом доступе. Далее, возможная анонимность цифровых каналов позволяет злоумышленнику защитить свою личность, что, как ему кажется, может помочь избежать юридических проблем, связанных с его действиями. Кроме того, цифровые каналы также позволяют злоумышленнику проводить одновременные веерные атаки на жертв, снижая затраты на проведение социоинженерных атак и увеличивая шансы найти жертву из-за эффекта масштаба. Отметим также, что в киберпространстве легче вызвать доверие, чем в физическом мире, потому что большинство людей полагаются на базовые эвристики, для принятия решения. Большинство людей опирается на внешние атрибуты при формировании доверия внешними атрибутами, такие как интерфейс веб-сайта или наличие разнообразного и обширного контента. Внешние атрибуты в интернет пространстве также могут создать видимость надежности, злоумышленник может включать в сообщения артефакты: ссылки, изображения, например, индикаторы безопасности, такие как висячие замки Secure Sockets Layer (SSL) или изображения организаций, которые подтверждают надежность человека.

Следует учитывать, что мотивация самих злоумышленников может отличаться высокой степенью разнообразности [14]. Наиболее распространённой целью выступает получение финансовой выгоды посредством хищения денежных средств или продажи конфиденциальной информации. Вместе с тем существуют и иные мотивы, такие как похищение данных с последующим использованием их для манипуляций или вымогательства, дестабилизация функционирования информационных систем, нанесение ущерба инфраструктуре жизненно-важных объектов с намерением вызвать панику и страх, преследование политических или идеологических целей, распространение ложной информации и пропаганда определенных взглядов, а также осуществление разведывательной деятельности. Помимо экономических и политических стимулов, важное значение имеют и психологические аспекты мотивации преступников, такие как стремление удовлетворить потребность в ощущении власти и контроля над ситуацией, а также желание добиться признания внутри специализированных сообществ, например, среди хакеров.

IV. УЯЗВИМОСТИ ЖЕРТВЫ

Задача потенциальной жертвы, чтобы защитить себя от негативных последствий, — выявить социоинженерные атаки, избегая при этом высокого уровня ложноположительных результатов. Чтобы предотвратить виктимизацию, получатель сообщения должен обработать его критически, обнаружить несоответствия и признаки обмана в сообщении. Атрибуты, способствующие этому, включают опыт, знание и бдительность. Люди с опытом имеют более точные ментальные модели угроз, которые улучшают оценку угроз и восприятие риска. Знания в предметной области можно приобрести посредством предыдущего негативного опыта, но лучше путем изучения особенностей, признаков и классов социоинженерных атак. Это помогает в распознавании образов и обнаружении обманчивых сигналов, отмечая при этом, что обнаружение обманных сигналов является предшественником подозрений. Бдительность — это процесс выделения когнитивных ресурсов для выполнения сложной задачи, например, обнаружения сигналов, которые могут указывать на обманные намерения в сообщении. Чтобы обнаружить признаки обмана в социоинженерной атаке, необходимо перенаправить свое внимание на обнаружение несоответствий в сообщении, причем несоответствия должны быть достаточно заметными, чтобы их можно было обнаружить. Стремление злоумышленников напугать жертву, ограничить во времени, использовать принцип дефицита приводит к активизации эмоциональной сферы, возрастанию тревожности, появлению страха, что притупляет бдительность и ограничивает возможности критического восприятия ситуации.

Угрозы, основанные на социальной инженерии, известны уже много лет, но они по-прежнему имеют высокие шансы на успех, поскольку тесно связаны с человеческой природой. Согласно Кевину Митнику, мы, как люди, все уязвимы перед обманом, потому что человек может изменить уровень доверия другого человека (или при соответствующей подготовке убрать недоверие), если правильно подобрать манипуляцию или серию манипуляций» [15].

Действительно, расследуя виктимизацию в случае с социоинженерными атаками, наблюдается, что отдельные личностные особенности могут играть активную роль в успехе атак социальной инженерии [16]. Кроме того, стресс, давление и другие факторы могут способствовать отсутствию контроля и гарантировать успех атаки.

Демографические, психосоциальные и эмпирические факторы выделяются как три наиболее важных фактора, связанных с восприимчивостью к фишингу [17]. Исследования дают противоречивые результаты относительно корреляции между демографическими факторами, такими как пол и возраст, и восприимчивостью к фишингу. Некоторые исследования утверждают, что женщины более подвержены фишинговым электронным письмам [18], в то время как другие сообщают, что нет существенных гендерных различий [19], [20] или даже предполагается, что мужчины могут быть более восприимчивы в определенных сценариях [21], [22]. Аналогичным образом наблюдались несоответствия в результатах, связанных с возрастом: большинство исследований показали, что молодые люди (в возрасте от 18 до 25 лет)

более склонны нажимать на фишинговые электронные письма по сравнению со старшими возрастными группами. Однако существуют и противоречивые результаты, в том числе исследования, предполагающие, что самая старшая возрастная группа (старше 59 лет) является наиболее восприимчивой или не сообщающие об отсутствии существенных возрастных различий в восприимчивости к фишингу среди студентов и преподавателей университетов [19]. В некоторых исследованиях говорится о роли уровня образования жертв в восприимчивости к социоинженерным атакам [16]. Центробанк России провёл уже традиционное ежегодное исследование в ноябре 2024 года, в котором приняли 429 063 физических лиц, и выявил основные характеристики жертв мошенников в 2024 году [23]. Чаще всего ими становятся работающие женщины (52,6% опрошенных) в возрасте от 25 до 44 лет со средним уровнем дохода и образования. Стоит отметить, что доля женщин незначительно больше доли мужчин, в отличие от 2023 года. Исследователи отмечают, что среди пострадавших увеличивается доля граждан старше 65 лет. В 2024 году примерно 33% опрошенных столкнулись с различными видами финансового мошенничества, и 9% потеряли деньги из-за действий злоумышленников. В 55% случаев ущерб не превышал 20 тысяч рублей, но это значение меньше, по сравнению с 2023 годом, а увеличилась доля хищений свыше 20 тысяч рублей. Более 40% пострадавших обратилась в свой банк по поводу кражи средств, в 2023 году таких людей была примерно треть. Уменьшилась доля телефонного мошенничества и с использованием смс, но в пятерку самых популярных у мошенников приемов впервые вошло получение доступа к аккаунту на Госуслугах.

Психосоциальные факторы включают психологические аспекты, такие как черты личности или межличностное поведение, которые могут повлиять на уязвимость человека к фишинговым атакам. В рамках «Большой пятерки» личностных качеств люди с более высоким уровнем открытости были более восприимчивы к социальной инженерии. Выявлена положительная связь между восприимчивостью к фишингу и доброжелательностью, при этом более высокий уровень нормативной приверженности, доверия и подчинения авторитету связан с большей вероятностью стать жертвой атак социальной инженерии. Обнаружена положительная корреляция между нейротизмом и восприимчивостью к фишинговым электронным письмам [19].

Также, с другой стороны, эффективны психологические принципы убеждения [24]. Злоумышленники для успешной реализации СИА могут использовать разнообразные методики социального влияния. Р. Чалдини выделяет шесть принципов социального влияния, он их еще называет оружием влияния. К ним относятся: взаимный обмен, приверженность и последовательность, социальное доказательство, симпатия, авторитет и дефицит. Принцип взаимного обмена гласит, что люди с большей вероятностью отвечают услугой на оказанную услугу, даже, если они об этом не просили. Также люди склонны проявлять последовательность и приверженность какой-то деятельности, если они эту деятельность уже начали или их в нее включили. Люди с большей охотой выполняют просьбы других людей, если они чувствуют сходство или признают авторитетность другого человека. Наконец, люди охотнее приобретают что-то, если воспринимают это как дефицитные вещи. Это оружие можно использовать для повышения успешности социоинженерной атаки. Например, ссылка, встроенная в сообщение, с большей вероятностью будет нажата, если будет обещано что-то хорошее (например, удвоение суммы пополнения баланса на телефон) или, наоборот, введено временное ограничение на маркетинговую акцию. Эти принципы часто комбинируются при осуществлении атаки злоумышленником. Злоумышленники изучают информацию, которая описывает, как методы атаки используют уязвимости человека, и объясняет, почему человеческие уязвимости приводят именно к таким последствиям атаки, а также, как методы атаки помогают достигать целей атаки. Таким образом, механизм воздействия, уязвимость человека и метод атаки могут служить тремя основными сущностями, позволяющими понять, как работают и действуют атаки социальной инженерии. В профилактических целях понимание сути и функций социоинженерных атак и повышение осведомленности пользователей информационных систем по этому вопросу должны быть включены в образовательные программы по кибербезопасности, уже начиная со школьного возраста.

V. Заключение

Проведенный анализ позволил глубже изучить природу социоинженерных атак и выявить ключевые факторы, способствующие их эффективному проведению. Актуальность темы обусловлена значительным ростом количества подобных инцидентов, высокой степенью успеха атак и значительной угрозой для информационной инфраструктуры организаций и индивидуальных пользователей. Исследование позволяет сделать ряд важных выводов.

Повышенная частота и разнообразие социоинженерных атак: за последние годы отмечается стабильный рост частоты подобных инцидентов, причем число успешных попыток увеличивается пропорционально общему количеству атак. Подобные инциденты наносят ощутимый экономический ущерб предприятиям, ведут к утрате важной коммерческой информации и снижают доверие клиентов и партнеров.

Использование доверия как основной вектор атаки: большая часть атак реализуется путём эксплуатации доверительных отношений, человек гораздо чаще оказывается вовлечен в схему обмана, если видит известное имя или бренд, ассоциирующийся с надежностью и честностью.

Недостаточная подготовка к распознаванию социоинженерной атаки: отсутствие должного уровня знаний о правилах безопасного обращения с информацией и способами идентификации опасных

сообщений создаёт благоприятные условия для атакующей стороны. Пользователи зачастую не осознают всю глубину рисков и не готовы оперативно реагировать на подозрительное взаимодействие.

Неготовность технических средств к решению проблемы: современные антиспам-системы и антивирусные программы оказываются бессильны против нападений, использующих социальную инженерию. Защита должна основываться на комбинации технического мониторинга и психологической готовности пользователей своевременно распознавать опасные сигналы.

Постоянная адаптация злоумышленников: регулярное изменение тактик и приемов социальной инженерии вынуждает специалистов непрерывно совершенствовать процедуры профилактики и повышать квалификацию сотрудников, занимающихся вопросами информационной безопасности.

Исходя из выводов, представляется необходимым сосредоточить усилия исследователей и практиков на следующих направлениях:

Изучение механизмов социальной инженерии: для эффективного противодействия атакам важно глубокое понимание используемых злоумышленниками схем и сценариев, включая психологические приемы давления, мотивацию преступников и характерные сценарии вовлечения жертв в противоправные действия.

Формирование концепции активной защиты: необходимы специальные программы обучения пользователей, способные развить практические навыки быстрого распознавания атак и своевременного уведомления должностных лиц о любых подозрительных событиях. Подобный подход позволит уменьшить долю удачных атак.

Адаптация политики информационной безопасности: руководству организаций рекомендуется пересмотреть политику безопасности с учетом новейших угроз, усилив процедуру проверки сообщений и активности пользователей, уделяя особое внимание предупреждению атак через электронную почту и телефоны.

Интеграция педагогических элементов в программы ИТ-обучения: внедрение курсов и тренингов, освещающих основы информационной гигиены и правила безопасной коммуникации, способно укрепить сопротивление сотрудника внешним социальным манипуляциям и снизить частоту случаев успешной атаки.

Применение автоматических аналитических систем: использование интеллектуальных аналитических платформ и машинного обучения для автоматического выявления аномалий в поведении пользователей повысит качество оперативного выявления угроз и снизит количество потенциальных уязвимых точек.

Таким образом, данная работа раскрывает сложность проблематики социоинженерных атак и предлагает целый набор шагов для минимизации рисков и увеличения устойчивости организаций и пользователей к подобному виду преступных деяний. Дальнейшие исследования будут направлены на разработку конкретных методов раннего выявления угроз и формирования эффективной стратегии информационной защиты.

Благодарности

Статья выполнена в рамках научно-исследовательской работы по государственному заданию СПб ФИЦ РАН Mol_Lab (молодежная_лаб) № FFZF-2024-0003.

Библиография

[1] Абрамов М.В., Тулупьев А.Л., Тулупьева Т.В. Психологические особенности, психические состояния пользователя и профиль его уязвимостей в контексте социоинженерных атак // Психология психических состояний: сб. статей студентов, магистрантов, аспирантов и молодых ученых. Казань, 2019. С. 312–317.

[2] May 2023 European Cybermarket News Report [Электронный ресурс] // European Cyber Security Organisation (ECSO). URL: https://ecs-org.eu/may-2023-european-cybermarket-news-report/ (дата обращения: 18.08.2025).

[3] Швыряев П.С. Киберпреступность как социальная проблема: стратегии противодействия: дис. ... канд. социол. наук. М.: МГУ им. М.В. Ломоносова, 2024. 189 с.

[4] Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. Т. 1. № 1. С. 18-27.

[5] Proofpoint: 70% директоров по кибербезопасности считают себя уязвимыми перед серьёзными кибератаками в 2024 году [Электронный ресурс] // CisoClub. URL: https://cisoclub.ru/proofpoint-70-direktorov-po-kiberbezopasnosti-schitajut-sebja-ujazvimymi-pered-serjoznymi-kiberatakami-v-2024-godu/ (дата обращения: 12.08.2025).

[6] Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: дис. ... д-ра юрид. наук. М.: Ун-т прокуратуры РФ, 2022. 557 с.

[7] Комлев Ю.Ю. Девиантность и преступность в эпоху high-tech, консьюмеризма и глэм-капитализма // Вестник КЮИ МВД России. 2018. № 1(31). С. 23-34. DOI: 10.24420/KUI.2018.31.11105.

[8] Комлев Ю.Ю. От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии // Российский девиантологический журнал. 2022. № 2(1). С. 17-26. DOI: 10.35750/27130622-2022-1-17-26.

[9] Краткая характеристика состояния преступности в Российской Федерации за январь - июнь 2025 года [Электронный ресурс] // МВД РФ. URL: https://мвд.рф/reports/item/67755056/ (дата обращения: 12.08.2025).

[10] Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.

[11] Тулупьева Т.В., Абрамов М.В., Тулупьев А.Л. Модель социального влияния в анализе социоинженерных атак // Управленческое консультирование. 2021. № 8. С. 97-107.

[12] Тулупьева Т.В., Абрамов М.В., Азаров А.А. Подходы к классификации социоинженерных атак // Информационное общество. 2025. № 3. С. 103-115. DOI: 10.52605/16059921_2025_03_103.

[13] Abramov M.V., Tulupyev A.L. Soft estimates of user protection from social engineering attacks: fuzzy combination of user vulnerabilities and malefactor competencies in the attacking impact success prediction // Artificial Intelligence and Natural Language. 2019. P. 47–58.

[14] Позднякова М.Е., Брюно В.В. Развитие информационно-сетевой среды и девиантное поведение: киберпреступность как новая социальная угроза // Вестник Института социологии. 2024. Т. 15. № 4. С. 235-254.

[15] Mitnick, K.D., Simon, W.L. The Art of Deception: Controlling the Human Element of Security. Indianapolis, IN: Wiley Publishing, Inc., 2002. 368 p.

[16] Jansen, J., Leukfeldt, R. How people help fraudsters steal their money: an analysis of 600 online banking fraud cases // Proceedings of the 5th Workshop on Socio-Technical Aspects in Security and Trust. 2015. P. 25–31.

[17] Fan, Z., Li, W., Laskey, K.B., Chang, K.-C. Investigation of Phishing Susceptibility with Explainable Artificial Intelligence // Future Internet. 2024. Vol. 16. Art. 31. DOI: 10.3390/fi16010031.
[18] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10). 2010. P. 373–382.
[19] Canfield, C., Fischhoff, B., Davis, A. Quantifying phishing susceptibility for detection and behavior decisions // Human Factors. 2016. Vol. 58. No. 8. P. 1158–1172.
[20] Iuga, C., Nurse, J.R.C., Erola, A. Baiting the hook: Factors impacting susceptibility to phishing attacks // Human-Centric Computing and Information Sciences. 2016. Vol. 6. Art. 8. DOI: 10.1186/s13673-016-0065-2.
[21] Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A. Correlating human traits and cyber security behavior intentions // Computers & Security. 2018. Vol. 73. P. 345–358.
[22] Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F. Social phishing // Communications of the ACM. 2007. Vol. 50. No. 10. P. 94–100.
[23] Киберпортрет региона - 2024 // Банк России. URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 18.08.2025).
[24] Cialdini, R.B. Influence: Science and Practice. 4th ed. Boston: Allyn and Bacon, 2000. 262 p.

Тулупьева Татьяна Валентиновна, канд. психол. наук, доцент, советник проректора Российской Академии народного хозяйства и государственной службы при Президенте Российской Федерации, Москва, ведущий научный сотрудник лаборатории прикладного искусственного интеллекта Санкт-Петербургского Федерального исследовательского центра Российской академии наук (https://dscs.pro/), Санкт-Петербург, email: tulupeva-tv@ranepa.ru, elibrary.ru: authorid=164301, ORCID: orcidID= 0000-0003-3630-7971.
Абрамов Максим Викторович, канд. техн. наук, руководитель лаборатории прикладного искусственного интеллекта Санкт-Петербургского Федерального исследовательского центра Российской академии наук (https://dscs.pro/), Санкт-Петербург, email: mva@dscs.pro, elibrary.ru: authorid=789095, ORCID: orcidID= 0000-0002-5476-3025.
Азаров Артур Александрович, канд. техн. наук, проректор по науке Российской Академии народного хозяйства и государственной службы при Президенте Российской Федерации (https://www.ranepa.ru/), Москва, email: azarov-aa@ranepa.ru, elibrary.ru: authorid= 621660, ORCID: orcidID= 0000-0003-3240-597X.

Social Engineering Attacks: Success Factors and Mitigation Strategies

Tatiana V. Tulupeva, Maksim V. Abramov, Artur A. Azarov

***Abstract*—This article examines the phenomenon of social engineering attacks, identifying key success factors and determining ways to enhance protection effectiveness. Our review of existing scientific literature demonstrates that social engineering attacks exhibit high adaptability and employ a broad spectrum of manipulation techniques, rendering traditional countermeasures insufficient. Particular attention is paid to the psychology of attackers, who exploit an understanding of human psychology to target cognitive and behavioral vulnerabilities. However, the primary focus remains on user vulnerability, emphasizing that the human factor is the key target, while technical measures play a secondary role. A significant research outcome is the identification of future scientific and practical directions. Developing integrated defense approaches is essential, combining technical measures with user awareness initiatives and cybersecurity training implementation. The application of specialized analytical systems, leveraging artificial intelligence technologies, is proposed as a promising tool for early threat detection and mitigation. Synthesizing the findings, the authors stress the importance of integrating disciplinary knowledge and combining expertise from diverse specialists to develop comprehensive defense strategies. Recommendations include strengthening information security personnel training, building sustainable employee competencies, and incorporating cybersecurity fundamentals into school curricula. This article lays the foundation for future research, innovation development, and implementation in information security practice, emphasizing the multifaceted and multidisciplinary nature of the challenges addressed.**

***Keywords*—Social engineering attack, user vulnerability, attacker, cyberattack, information system.**

REFERENCES

[1] M.V. Abramov, A.L. Tulupev and T.V. Tulupeva, "Psychological characteristics, mental states of the user and their vulnerability profile in the context of social engineering attacks," In *Psychology of Mental States: collection of articles by students, undergraduates, postgraduates and young scientists*, Kazan, pp. 312–317, 2019.

[2] *May 2023 European Cybermarket News Report*, European Cyber Security Organisation (ECSO) [Online]. Available: https://ecs-org.eu/may-2023-european-cybermarket-news-report/.

[3] P.S. Shviryaev, "*Cybercrime as a Social Problem: Counteraction Strategies*," dis. ... Cand. of Sociol. Sci, M., Lomonosov Moscow State University, 189 p., 2024.

[4] S.S. Vitvitskaya, A.A. Vitvitsky and Yu.I. Isakova, "Cybercrime: concept, classification, international counteraction," *Legal Order and Legal Values*, Vol. 1, No. 1, pp. 18-27, 2023.

[5] *Proofpoint: 70% of Chief Information Security Officers Consider Themselves Vulnerable to Serious Cyber Attacks in 2024*, CisoClub [Online]. Available: https://cisoclub.ru/proofpoint-70-direktorov-po-kiberbezopasnosti-schitajut-sebja-ujazvimymi-pered-serjoznymi-kiberatakami-v-2024-godu/.

[6] K.N. Evdokimov, "*Countering Computer Crime: Theory, Legislation, Practice*," dis.... Dr. of Jurid. Sci, M., University of the Prosecutor's Office of the Russian Federation, 557 p., 2022.

[7] Yu.Yu. Komlev, "Deviance and crime in the era of high-tech, consumerism and glam-capitalism," *Bulletin of the Kyui MIA of Russia*, No. 1(31), pp. 23-34, 2018, doi: 10.24420/KUI.2018.31.11105.

[8] Yu.Yu. Komlev, "From the digitalization of society to cybercrime, cyberdeviance and the development of digital deviantology," *Russian Deviantological Journal*, No. 2(1), pp. 17-26 2022, doi: 10.35750/27130622-2022-1-17-26.

[9] *Brief Overview of the State of Crime in the Russian Federation for January - June 2025*, Ministry of Internal Affairs of the Russian Federation (MVD RF) [Online]. Available: https://мвд.рф/reports/item/67755056/.

[10] A.A. Azarov, T.V. Tulupeva, A.V. Suvorova, A.L. Tulupev, M.V. Abramov and R.M. Yusupov, "Social Engineering Attacks," In *Analysis Problems*, St. Petersburg, Nauka, 352 p., 2016.

[11] T.V. Tulupeva, M.V. Abramov and A.L. Tulupev, "A model of social influence in the analysis of social engineering attacks," *Administrative Consulting*, No. 8, pp. 97-107, 2021.

[12] T.V. Tulupeva, M.V. Abramov and A.A. Azarov, "Approaches to the classification of social engineering attacks," *Information Society*, No. 3, pp. 103-115, 2025, doi: 10.52605/16059921_2025_03_103.

[13] M.V. Abramov and A.L. Tulupev, "Soft estimates of user protection from social engineering attacks: fuzzy combination of user vulnerabilities and malefactor competencies in the attacking impact success prediction," *Artificial Intelligence and Natural Language*, P. 47–58, 2019.

[14] M.E. Pozdnyakova and V.V. Bryuno, "Development of the information-network environment and deviant behavior: cybercrime as a new social threat." *Bulletin of the Institute of Sociology*, Vol. 15, No. 4, pp. 235-254, 2024.

[15] K.D. Mitnick and W.L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Indianapolis, Wiley Publishing, Inc., 368 p., 2002.

[16] J. Jansen and R. Leukfeldt, "How people help fraudsters steal their money: an analysis of 600 online banking fraud cases," In *Proceedings of the 5th Workshop on Socio-Technical Aspects in Security and Trust*, pp. 25–31, 2015.

[17] Z. Fan, W. Li, K.B. Laskey and K.-C. Chang, "Investigation of Phishing Susceptibility with Explainable Artificial Intelligence," *Future Internet*, Vol. 16, Art. 31, 2024, doi: 10.3390/fi16010031.

[18] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor and J Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*, pp. 373–382, 2010.

[19] C. Canfield, B. Fischhoff and A. Davis, "Quantifying phishing susceptibility for detection and behavior decisions," *Human Factors*, Vol. 58, No. 8, pp. 1158–1172, 2016.

[20] C. Iuga, J.R.C. Nurse and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," *Human-Centric Computing and Information Sciences*, Vol. 6, Art. 8, 2016, doi: 10.1186/s13673-016-0065-2.

[21] M. Gratian, S. Bandi, M. Cukier, J. Dykstra and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Computers & Security*, Vol. 73, pp. 345–358, 2018.

[22] T.N. Jagatic, N.A. Johnson, M. Jakobsson and F. Menczer, "Social phishing," *Communications of the ACM*, Vol. 50, No. 10, pp. 94–100, 2007.

[23] *Cyber Portrait of the Region – 2024*, Bank of Russia [Online]. Available: https://cbr.ru/statistics/information_security/cyber_portrait/2024.

[24] R.B. Cialdini, *Influence: Science and Practice*. 4th ed. Boston, Allyn and Bacon, 2000. 262 p.

Tatyana V. Tulupeva, PhD in Psychology, Associate Professor, Advisor to the Vice-Rector for Science, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow; Leading Research Scientist, Laboratory of Applied Artificial Intelligence, St. Petersburg Federal Research Center of the Russian Academy of Sciences (https://dscs.pro/), St. Petersburg, email: tulupeva-tv@ranepa.ru, elibrary.ru: authorid=164301, ORCID: orcidID=0000-0003-3630-7971.

Maksim V. Abramov, PhD in Engineering, Head of the Laboratory of Applied Artificial Intelligence, St. Petersburg Federal Research Center of the Russian Academy of Sciences (https://dscs.pro/), St. Petersburg, email: mva@dscs.pro, elibrary.ru: authorid=789095, ORCID: orcidID=0000-0002-5476-3025.
Artur A. Azarov, PhD in Engineering, Vice-Rector for Science, Russian Presidential Academy of National Economy and Public Administration (RANEPA) (https://www.ranepa.ru/), Moscow, email: azarov-aa@ranepa.ru, elibrary.ru: authorid=621660, ORCID: orcidID=0000-0003-3240-597X.