МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2025.153.121

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Научная статья

Диреев И.Д.[1, *]

[1] ORCID : 0009-0008-3669-7774;

[1] Южно-Уральский государственный университет (национальный исследовательский университет), Челябинск, Российская Федерация

* Корреспондирующий автор (tifey[at]udm.ru)

Аннотация

Социальная инженерия представляет собой одну из самых серьезных угроз для безопасности информации. В условиях растущей частоты кибератак осознание принципов социальной инженерии и способов защиты от неё становится особенно важным. В отличие от стандартных технических атак, при которых хакеры эксплуатируют недостатки программного обеспечения, методы социальной инженерии ориентированы на слабости людей, что делает их особенно опасными. Сегодня эта угроза особенно актуальна, поскольку даже наиболее защищенные организации могут стать уязвимыми из-за ошибки одного сотрудника. Целью данного исследования является анализ современных методов социальной инженерии (2022–2024 гг.), оценка их эволюции под влиянием технологий искусственного интеллекта и разработка комплексного подхода к противодействию. На основе анализа данных выявлены ключевые тенденции: рост фишинга на 50% в 2024 году, увеличение ущерба от вишинга до 250 млрд рублей, использование дипфейков. Результаты исследования включают классификацию атак, оценку эффективности законодательных мер и практические рекомендации, сочетающие технологические решения (нейросети, поведенческая аналитика) с обучением персонала. Новизна исследования заключается в интеграции данных о российском киберпространстве и прогнозе развития атак с применением искусственного интеллекта на 2025 год.

Ключевые слова: социальная инженерия, фишинг, искусственный интеллект в кибербезопасности, поведенческая аналитика, информационная безопасность дипфейки.

SOCIAL ENGINEERING IN THE CONTEXT OF INFORMATION SECURITY

Research article

Direev I.D.[1, *]

[1] ORCID : 0009-0008-3669-7774;

[1] South Ural State University (National Research University), Chelyabinsk, Russian Federation

* Corresponding author (tifey[at]udm.ru)

Abstract

Social engineering is one of the most serious threats to information security. With the increasing frequency of cyber-attacks, awareness of the principles of social engineering and ways to protect against it is becoming especially important. Unlike standard technical attacks, in which hackers exploit software flaws, social engineering methods are focused on people's weaknesses, which makes them especially dangerous. This threat is especially relevant today, as even the most secure organizations can become vulnerable due to a mistake by one employee. The purpose of this study is to analyze modern methods of social engineering (2022-2024), assess their evolution under the influence of artificial intelligence technologies and develop an integrated approach to counteraction. Based on the data analysis, key trends have been identified: a 50% increase in phishing in 2024, an increase in vishing damage to 250 billion rubles, and the use of deep fakes. The research results include a classification of attacks, an assessment of the effectiveness of legislative measures, and practical recommendations combining technological solutions (neural networks, behavioral analytics) with staff training. The novelty of the research lies in the integration of data on Russian cyberspace and the forecast of the development of attacks using artificial intelligence for 2025.

Keywords: social engineering, phishing, artificial intelligence in cybersecurity, behavioral analytics, information security, deep fakes.

Введение

Социальная инженерия – это способ воздействия на людей с целью получения строго конфиденциальной информации или обхода технических средств защиты для доступа к системам. Угроза социальной инженерии особенно актуальна, поскольку даже наиболее защищенные организации могут становиться уязвимыми из-за ошибки одного сотрудника. Суть социальной инженерии заключается в применении психологических манипуляций, которые эксплуатируют эмоции и доверие жертвы для реализации замыслов преступника. Согласно информации от Positive Technologies, в 2024 году примерно 50% успешных кибератак на компании осуществлялись с использованием техник социальной инженерии [1], что подчёркивает важность изучения этого явления.

Цель данной статьи – описать основные формы социальной инженерии, разработать стратегию противодействия на основе анализа современных атак (2022–2024 гг.) и прогноза их развития, для предотвращения данных угроз.

Задачи:

1. Классифицировать методы социальной инженерии с учетом новых технологий (искусственный интелект, дипфейки).

2. Оценить эффективность законодательных инициатив РФ (2023-2024 гг.).

3. Предложить модель обучения персонала, интегрированную с системами AI-аналитики.

Научная новизна заключается в комбинации поведенческого анализа и AI-моделей для прогнозирования атак, а ***практическая значимость*** – в адаптации рекомендаций под специфику российского киберпространства.

Социальная инженерия, трансформируясь под влиянием цифровых технологий, перешла от примитивного фишинга к сложным гибридным атакам с использованием искусственного интеллекта. Работы Hadnagy (2010) и Mitnick (2002) заложили основы понимания психологических механизмов социальной инженерии [2], [3], однако цифровая трансформация 2020-х годов требует переоценки рисков. Если в 2010-х годах исследования, рассматривали социальную инженерию как проблему человеческой доверчивости [4], [5], то в 2024 году, по данным IBM X-Force, 63% атак включают элементы генеративного искусственного интелекта, включая дипфейки и синтез голоса [6]. В России, по данным «Сбера», ущерб, нанесенный «телефонными мошенниками» в 2024 году гражданам Российской Федерации, составил сумму не менее 250 миллиардов рублей [7], что ставит вопрос о необходимости пересмотра классических моделей кибербезопасности.

Исследователи называют социальную инженерию одной из самых серьёзных проблем десятилетия и подчеркивают роль искусственного интеллекта в персонализации атак [8]. Владение навыками социальной инженерии будет приобретать всё большее значение для организаций и государств из-за влияния на геополитику. Также социальная инженерия ставит под сомнение верность принимаемых нами решений, так как они могут основываться на искусственных и предвзятых источниках информации [9].

Примеры потенциальных угрозы социальной инженерии для организаций и частных лиц:

- утрата конфиденциальности персональных данных;
- утрата финансовых средств или платежной информации;
- утрата конфиденциальной информации компании;
- компрометация паролей сотрудников;
- несанкционированный доступ к базам данных пользователей или клиентов организации;
- заражение устройств вредоносным программным обеспечением (ПО), с возможным дальнейшими последствиями, типа полного сбоя работы организации или производства;
- коммерческая разведка;
- использование взломанных учетных записей для осуществления дальнейших атак с применением методов социальной инженерии от имени взломанной компании или лица.

Основные атаки, применяемые при помощи методов социальной инженерии

2.1. Фишинг

Фишинг является наиболее распространённым методом мошенничества, при котором преступники создают фальшивые веб-сайты или рассылают электронные письма, выглядящие как настоящие. С помощью манипулятивных приёмов они стремятся убедить жертв перейти по опасным ссылкам. Основная задача – вынудить пользователей раскрыть свои личные данные. Также распространена схема с имитацией писем от банков, где вас просят обновить данные учетной записи из-за «подозрительной активности» [10].

По данным экспертов, в 2024 году в России было зафиксировано свыше 350 тысяч фишинговых веб-ресурсов, что на 50% превышает показатели прошлого года, когда было зарегистрировано 210 тысяч таких ресурсов. Прогнозируется, что в 2025 году эта отрицательная динамика сохранится. Специалисты связывают это с ростом цифровизации в бизнесе, низким барьером для входа мошенников и легкостью создания фишинговых платформ [11].

Примеры фишинга:

Среди наиболее распространенных схем в России можно отметить: взлом аккаунтов в Telegram (свыше 40 тысяч случаев), подделку сайтов, предлагающих мгновенные выплаты (свыше 80 тысяч, чаще всего это онлайн казино, лотереи и другие инвестиционные платформы), а также интернет-сервисов для размещения объявлений и маркетплейсов (свыше 20 тысяч) [11].

В 2022 году стало известно о проведении атаки на Uber. Восемнадцатилетнему хакеру удалось взломать несколько систем компании. Все началось с того, что злоумышленник нашел логин и пароль одного из подрядчиков Uber в даркнете и начал отправлять подрядчику множество запросов на аутентификацию, создавая тем самым спам-атаку. Затем хакер связался с ним через WhatsApp, выдав себя за сотрудника техподдержки, и предложил решение проблемы: для прекращения спама нужно просто подтвердить запрос. Так, при помощи методов социальной инженерии, хакер обошел многофакторную аутентификацию и получил доступ к внутренней сети Uber через корпоративный VPN [12].

Следует обратить особое внимание на методику атаки, известную как Business Email Compromise, которая в последние годы стала весьма распространенной. Эта техника, называемая угоном разговора (Conversation Hijacking) [12], направлена на вмешательство в уже существующую переписку, при этом злоумышленник выдает себя за одного из участников. Обычно для этого не требуется взлом аккаунтов или использование технических средств для маскировки отправителя; достаточно получить реальное сообщение и создать похожий домен. Это позволяет преступникам быстро завоевать доверие остальных собеседников и незаметно направлять разговор в нужное им русло. Часто для таких атак используются базы данных электронной почты, которые продаются в даркнете, и их источником становятся взломы или утечки информации.

Ярким примером угонов беседы является инцидент, связанный с трансфером футболиста Леандро Паредеса [13]. Злоумышленники смогли вмешаться в переписку, представляясь сотрудником клуба Boca Juniors, который ожидал получить небольшой процент от суммы сделки – 520 тысяч евро. В итоге именно эту сумму мошенники и присвоили.

Одним из наиболее значительных случаев подобных атак стало преступление, совершенное литовцем Эвалдасом Римасаускасом против двух крупнейших мировых интернет-компаний: Google и Facebook. Римасаускас со своей командой создали фиктивную компанию, представляясь производителем компьютерной техники, который сотрудничал с этими гигантами. Кроме того, они открыли банковские счета на имя этой компании. По данным Министерства юстиции США, в результате этой схемы интернет-гиганты понесли убытки, превышающие 120 миллионов долларов [14].

2.2. Претекстинг

Претекстинг – представляет собой форму мошенничества, которая обычно осуществляется через мобильные устройства. В этом процессе злоумышленник использует заранее подготовленный текст или сценарий, чтобы побудить потенциальную жертву к определённым действиям или получить конфиденциальные данные, необходимые для кражи денег у граждан [15]. Для того чтобы снизить подозрительность, мошенники прибегают к созданию фальшивых аккаунтов, электронных почтовых адресов и телефонных номеров, а также используют видео и аудио, сгенерированные искусственным интеллектом. Основной целью таких атак чаще всего становятся финансовые данные, включая номера банковских карт, ПИН-коды и CVV-коды, а также средства на счетах.

Также злоумышленники используют технику, называемую вишингом, или голосовым фишингом. Этот метод заключается в том, что преступники звонят жертвам с целью выманивания их личных данных. Этот метод стал особенно актуальным на фоне роста цифровых технологий и продолжает набирать популярность. В некоторых случаях термины «претекстинг» и «вишинг» используются как синонимы, или же претекстинг рассматривается как одна из форм вишинга [16].

Примеры претекстинга (вишинга):

1. Схема «родственник в беде»:

- мошенник может притвориться вашим родственником или знакомым и с паническим голосом сообщить, что попал в ДТП или оказался под следствием за какое-либо тяжкое преступление;
- кроме того, он может выдать себя за представителя силовых ведомств, который якобы помогает вашему близкому в решении возникшей проблемы;
- для разрешения этой «ситуации» злоумышленники обычно требуют определённую сумму денег, которую необходимо доставить в указанное место или передать какому-либо человек [17].

2. Схема от имени сотрудника банка:

- злоумышленники уведомляют жертву о попытке осуществления перевода крупной суммы денег с её банковского счета. Если жертва хочет отменить перевод, мошенники требуют предоставить данные карты или секретный код, полученный в SMS;
- аферисты могут позвонить жертве после получения пластиковой карты и, выдавая себя за представителей банка, предложить её активировать. В процессе общения они выманивают информацию о банковской карточке;
- жертве могут предложить кредит на подозрительно привлекательных условиях от имени банка, после чего злоумышленники просят оплатить комиссионные сборы или внести деньги для оформления страховки по кредиту [18].

3. Схема мошенничества с использованием сотрудников силовых ведомств и других государственных учреждений выглядит следующим образом:

- злоумышленники информируют жертву о том, что ее банковские средства находятся под угрозой кражи;
- после этого они предлагают ей снять деньги и перевести их на «безопасный» счет;
- часто жертву убеждают взять кредит, чтобы предотвратить действия «воров», то есть чтобы не превышать так называемый «кредитный лимит»;
- в ходе беседы мошенники используют авторитетные названия должностей, оказывают давление, спешат и запугивают жертву, угрожая серьезными последствиями за отказ сотрудничать [19].

4. Использование искусственного интеллекта:

- с применением искусственного интеллекта злоумышленники способны воспроизвести голос, например генерального директора компании и направить голосовое сообщение с просьбой перевести значительную сумму денег на указанный счёт;
- фальшивые видеоконференции – руководитель компании «появляется» на видеозвонке и даёт распоряжения сотрудникам, хотя на самом деле это подделка.

С целью борьбы с телефонным мошенничеством, 26 декабря 2024 года Правительство Российской Федерации приняло Постановление [20], которое вводит ограничения на звонки через IP-телефонию. Данная технология позволяла пользователям интернета связываться с абонентами стационарных и мобильных телефонов, а также подменять номера. По информации Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, теперь этот вид мошенничества будет значительно затруднён, так как будет исключена возможность подключения сетей передачи данных к телефонным сетям [20].

Также принятый 24 июля 2023 года Федеральный закон Российской Федерации [21] позволил банкам замораживать деньги после выявления подозрительных операций, что усложнило проведение банковских мошенничеств злоумышленниками.

2.3. Бэйтинг (приманка)

Бэйтинг привлекает внимание жертв с помощью различных приманок. Такой приманкой может служить зараженная вредоносным программным обеспечением USB-накопитель, оставленный в общественном месте. В онлайн-среде приманки могут принимать форму привлекательной рекламы или заманчивых предложений, которые ведут на вредоносные сайты или предлагают установить вредоносные приложения [22]. Особенность бейтинга заключается в том, что жертва выполняет запросы злоумышленников добровольно, например, из-за любопытства или из-за жадности.

Примеры бэйтинга:

Мошенники размещают рекламу с привлекательными предложениями, например, «бесплатные фильмы» или «специальные скидки». При клике на такую рекламу пользователь перенаправляется на вредоносный сайт или скачивает заражённое приложение.

В одном исследовании, опубликованном в 2016 году, исследователи разбросали 297 USB-накопителей по территории кампуса Иллинойсского университета. На накопителях были файлы, которые ссылались на веб-страницы, принадлежащие исследователям. Исследователи смогли увидеть, на скольких накопителях были открыты файлы, но не смогли определить, сколько накопителей было вставлено в компьютер без открытых файлов. Из 297 дисков, которые были утеряны, 290 (98%) были найдены, а 135 (45%) из них «вернулись домой» [23].

2.4. Обратная социальная инженерия

Обратная социальная инженерия – это техника манипулирования, при которой человека обманом вынуждают самостоятельно связаться со злоумышленником. В результате между жертвой и хакером возникает высокая степень доверия, так как пользователь начал общение сам.

Пример обратной социальной инженерии:

Установка программ-вымогателей на компьютеры пользователей представляет собой разновидность вредоносного ПО, целью которого является вымогательство. Эти программы могут блокировать доступ к системе или мешать чтению сохраненных данных, зачастую применяя методы шифрования, и требуют от жертвы уплаты выкупа для восстановления прежнего состояния.

Существует несколько типов программ-вымогателей:

- шифровальщики – они шифруют файловую систему на компьютере жертвы и требуют деньги за предоставление ключа для расшифровки;
- блокировщики – такие программы блокируют устройство или экран, запрашивая оплату для восстановления доступа;
- запугиватели (Scareware) – это фальшивые антивирусные программы и другие виды ПО, которые предупреждают пользователей о том, что их устройство заражено вирусной программой или другим вредоносным ПО.

2.5. Водопой

Водопой представляет собой изощренный метод киберугроз, целью которого является компрометация определенной группы людей, основываясь на их привычках в интернет-серфинге. Злоумышленники выбирают сайты, которые часто посещают их жертвы, такие как корпоративные страницы, специализированные порталы или другие ресурсы, которым жертвы доверяют.

Во время подготовки к атаке злоумышленники анализируют слабые места этих веб-ресурсов, что дает им возможность внедрять вредоносные скрипты, чаще всего это JavaScript или непосредственно в HTML-код страниц. Как только пользователь посещает скомпрометированный ресурс, вредоносное ПО запускается, что приводит к установке дополнительных вирусов на компьютер или к его захвату преступниками.

Такой подход особенно эффективен против сотрудников компаний или государственных корпораций, поскольку они могут быть более уязвимы к атакам, направленным на конкретные ресурсы, с которыми они работают ежедневно. Этот метод атак подчеркивает важность защиты сайтов и сетевой безопасности, а также необходимость осведомленности пользователей о возможных угрозах.

2.6. Социальная маскировка

Этот метод связан с выдачей злоумышленника за доверенное лицо, например, сотрудника технической поддержки или менеджера компании

Пример социальной маскировки: недоброжелатель проник в офис организации под видом курьера, произвёл подмену реального роутера на модифицированное устройство и заполучил полный контроль над сетью.

Цикл атак социальной инженерии и стратегии защиты

Пример четырехступенчатого цикла социальной инженерии:

1) подготовка: на начальном этапе злоумышленник аккумулирует как можно больше информации о своей жертве или компании, изучает особенности ее работы и внутренние процессы. Он фиксирует все детали, которые будут полезны для последующего проникновения. Полученная информация используется для установления контакта на следующем этапе;

2) проникновение: мошенник начинает общение с выбранной целью, применяя методы социальной инженерии, и стремится завоевать доверие, представляясь другим лицом;

3) эксплуатация: ключевая цель всей схемы – заставить жертву выполнить «целевое действие». Это может быть, например, переход по вредоносной ссылке в электронном письме, ввод конфиденциальных данных в форму на внешнем ресурсе или открытие архива, содержащего вредоносное ПО, прикрепленного к письму;

4) завершение: после выполнения жертвой целевого действия мошенник прекращает общение (в случае фишинговых писем обратная связь изначально не предполагается). Злоумышленник получил то, что ему нужно, и теперь будет использовать собранные данные в своих интересах.

Если злоумышленник не смог добиться успеха с первой попытки, это не означает его поражения. Чаще всего он будет пробовать новые подходы, чтобы «подобрать ключ» к своей жертве.

По данным от Positive Technologies, российской компании, специализирующаяся на разработке решений в сфере информационной безопасности, в 2024 году электронная почта остается главным инструментом социальной инженерии для организаций, составляя 88%, в то время как для частных пользователей основным ресурсом являются сайты с показателем 73%. Злоумышленники активно эксплуатируют популярность социальных сетей среди индивидуальных пользователей для осуществления кибератак. В сравнении с предыдущим кварталом, использование этого метода возросло на 4%. Наиболее предпочтительной социальной сетью среди преступников стал Facebook.

По данным Генеральной прокуратуры Российской Федерации, за первые 11 месяцев 2024 года значительная часть всех мошенничеств (85%, или 350 тысяч случаев) была совершена с использованием информационно-телекоммуникационных технологий и в области компьютерной информации. К ним относятся мошенничества с подменой телефонных номеров, интернет-мошенничества, мошенничества с платежными системами и другие виды кибермошенничества. За 11 месяцев 2024 года общее количество их увеличилось на 7,8%. В целом преступления в сфере IT-технологий и компьютерной информации составляют почти 40% от всех зарегистрированных правонарушений (702,9 тысячи, рост за год на 14,3%) [24].

Необходимые мероприятия для предотвращения атак с использованием социальной инженерии в организации:

1. Обучение персонала. Систематическое и регулярное информирование сотрудников на всех уровнях и в каждом отделе о типах атак и психологических приемах, которые используют злоумышленники для получения необходимых данных.

2. Тренировки на проникновение. Специалисты по информационной безопасности советуют представителям IT-отделов регулярно проводить тренировки на уязвимости к атакам с применением методов социальной инженерии. Это позволит специалистам выяснить, какие из пользователей более подвержены определённым атакам. Тренировка на проникновение представляет собой искусственно созданную кибератаку на компьютерную систему или отдельных пользователей с целью проверки наличия слабых мест. Регулярные тесты позволяют оценить готовность сотрудников и протестировать потенциальные масштабы утечки данных. Имитацию фишинговых атак можно проводить с использованием специализированного ПО. Во время этих тренировок сотрудникам присылаются фишинговые письма, что помогает выяснить, кто из них поддается методам социальной инженерии. После этого такие сотрудники должны пройти дополнительное обучение.

3. Внедрение строгих процедур. Двухфакторная аутентификация (2FA) представляет собой метод, который требует два различных способа для подтверждения вашей идентичности. К примеру, это может быть сочетание пароля и кода, полученного на ваш мобильный телефон. 2FA считается одним из самых надежных способов защиты от атак, использующих приемы социальной инженерии.

4. Разграничение доступа к защищаемой информации. Сотрудники должны иметь доступ только к той информации, которая необходима для выполнения их работы.

5. Использование защиты от вредоносного программного обеспечения. Необходимо применять комплексный подход, который включает антивирусные решения для интернет-серфинга, защиту электронной почты и антивирусные программы для борьбы со шпионскими приложениями. Некоторые компании предлагают интегрированные решения, но также можно использовать несколько качественных продуктов от разных производителей. Главная задача данной защиты заключается в том, чтобы остановить нежелательные действия, возникающие, когда пользователи переходят по ссылкам в электронных письмах и мессенджерах. Если пользователь нажмет на ссылку (в браузере, почтовом клиенте или мессенджере), и открывшаяся веб-страница будет вызывать подозрения в отношении сетевых угроз, защитная система обязана заблокировать доступ к этой странице, содержащей вредоносный контент.

6. Регулярные обновления операционной системы. Все компьютеры в организации должны своевременно получать обновления, так как разработчики периодически выпускают патчи, необходимые для устранения выявленных уязвимостей.

7. Правильный выбор и регулярная замена паролей. Для повышения безопасности организациям следует установить строгие правила управления паролями. Сотрудники должны регулярно обновлять свои пароли и, что особенно важно, создавать их правильно. Наилучшим решением являются сгенерированные пароли, которые крайне трудно угадать. Кроме того, важным моментом является обучение сотрудников методам безопасного хранения таких паролей.

8. Применение брандмауэра. Качественный сетевой фаервол способен блокировать вредоносные запросы, включая атаки, основанные на методах социальной инженерии. Таким образом, прежде чем пользователи попадут на ваш сайт, они проходят фильтрацию через сетевой фаервол, который определяет безопасность подключения и блокирует его, если оно выглядит как мошенническое.

9. Использование искусственного интеллекта. Использование нейронных сетей и алгоритмов обработки естественного языка (NLP) для защиты от фишинговых атак является эффективным способом борьбы с мошенничеством в сфере онлайн-банкинга. Данные технологии позволяют выявлять и блокировать фишинговые сообщения и сайты, что дает возможность банкам обезопасить своих клиентов от возможных опасностей. Также алгоритмы машинного обучения могут быть тренированы с использованием исторических данных о поведении пользователей и обычных транзакциях. Это позволяет обнаруживать аномалии или необычные действия и шаблоны, которые могут сигнализировать о возможных рисках для безопасности.

10. Системы анализа поведения. Поведенческая аналитика позволяет обнаруживать подозрительные активности, такие как доступ к системе с незнакомого устройства или необычное использование информации.

11. Современная организация пропускного режима. Гарантия физической безопасности, включая организации охраны, внедрения пропускной системы, установки камер видеонаблюдения, сигнализации и контроля доступа к устройствам, способствует предотвращению несанкционированного доступа злоумышленников на защищенную территорию.

12. Создание благоприятной обстановки. Работники должны ощущать уверенность и не бояться делиться своими подозрениями, если у них есть основания полагать, что они стали жертвами социальной инженерии. Тем не менее, они не станут этого делать, если будут опасаться последствий или осуждения со стороны своих коллег. Это имеет большое значение, так как оперативное информирование о подобных инцидентах помогает быстро нейтрализовать угрозу до того, как компании будет нанесён серьёзный ущерб.

Для эффективного противодействия социальной инженерии необходим комплексный подход, в котором технологии и человеческий аспект дополняют друг друга. Защита от социальной инженерии представляет собой сложную задачу, поскольку она нацелена не только на технические средства, но и на человеческие слабости. Даже самые защищенные системы могут оказаться под угрозой, если человек, отвечающий за их использование, станет жертвой манипуляций. Технические решения, такие как антивирусные программы и межсетевые экраны, окажутся неэффективными против фальшивого звонка или письма, если пользователь не сможет своевременно распознать опасность [25].

Прогноз развития алгоритмов социальной инженерии в 2025 году от компании – отечественного разработчика системы автоматизированного управления знаниями сотрудников в области кибербезопасности [26]:

- широкое применение искусственного интеллекта (ИИ) для персонализации кибератак в реальном времени. ИИ будет способствовать злоумышленникам в настройке атак, делая их более целенаправленными и убедительными;
- увеличение числа атак с использованием дипфейков и фальшивого медиа-контента, поддельные звонки и видеосообщения будут применяться для создания иллюзии доверия;
- рост количества персонализированных атак на отдельных лиц. Жертвы будут выбираться на основе анализа их социальных связей, общественной активности и личной информации;
- преобладание мессенджеров как главной платформы для мошеннических действий. Мессенджеры продолжат оставаться основными инструментами для атак из-за их широкой популярности и сложности в отслеживании;
- активное использование технологии для обхода современных мер защиты и выявления угроз. Злоумышленники будут шире применять инновационные методы, чтобы сократить риск обнаружения.

Заключение

Социальная инженерия остаётся одним из наиболее опасных вызовов в сфере информационной безопасности, трансформируясь под влиянием цифровых технологий и ИИ. Проведённое исследование выявило ключевые тенденции 2022–2024 гг.: рост фишинга на 50%, увеличение ущерба от вишинга до 250 млрд рублей, а также активное внедрение дипфейков и генеративного ИИ в атаки. Эти методы, эксплуатирующие человеческий фактор, демонстрируют, что даже технически защищённые системы уязвимы из-за ошибок персонала.

Анализ современных атак подтвердил, что 63% инцидентов включают элементы ИИ, что подчёркивает необходимость пересмотра классических моделей защиты. Законодательные инициативы РФ (ограничение IP-телефонии, заморозка подозрительных транзакций) показали умеренную эффективность, однако их недостаточно для противодействия быстро эволюционирующим угрозам.

В качестве решения предложен комплексный подход, сочетающий технологические инновации (нейросети для анализа поведения, NLP-алгоритмы для детектирования фишинга) с регулярным обучением сотрудников. Особое значение имеет интеграция симуляций атак и поведенческой аналитики, позволяющая минимизировать риски человеческого фактора. Новизна исследования заключается в адаптации рекомендаций к специфике российского киберпространства и прогнозе на 2025 год, где ожидается рост персонализированных атак через мессенджеры, использование дипфейков и ИИ-оптимизированных сценариев.

Практическая значимость работы подтверждается разработкой модели, объединяющей превентивные меры (обновление законодательства, строгие процедуры аутентификации) и предиктивные технологии. Для устойчивости к социальной инженерии критически важно сочетать технические решения с формированием «культуры безопасности» среди сотрудников, где доверие и оперативное информирование об угрозах становятся основой защиты.

Конфликт интересов

Не указан.

Рецензия

Артамонов В.А., Международная академия информационных технологий (МНОО "МАИТ), Минск, Беларусь

DOI: https://doi.org/10.60797/IRJ.2025.153.121.1

Conflict of Interest

None declared.

Review

Артамонов V.A., International Academy of information technologies, Minsk, Belarus

DOI: https://doi.org/10.60797/IRJ.2025.153.121.1

Список литературы / References

1. Беседина В. Актуальные киберугрозы: III квартал 2024 года / В. Беседина. — 2024. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id1 (дата обращения: 10.01.2025).
2. Hadnagy C. Social Engineering: The Art of Human Hacking / C. Hadnagy. — Indianapolis : Wiley, 2010. — 384 p.
3. Mitnick K. The Art of Deception: Controlling the Human Element of Security / K. Mitnick. — Hoboken : John Wiley & Sons, 2011. — 368 p.
4. Mitnick K. Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker / K. Mitnick. — New York : Little, Brown and Company, 2011. — 432 p.
5. Hadnagy C. Social Engineering: The Science of Human Hacking / C. Hadnagy. — 2nd ed. — Hoboken : John Wiley & Sons, 2018. — 368 p.
6. IBM X-Force Threat Intelligence Index 2024. — Armonk : IBM, 2024. — URL: https://www.ibm.com/reports/threat-intelligence (accessed: 18.02.2025).

7. В Сбере сообщили, что ущерб от мошенников составил 250 млрд руб. в 2024 году // Вести. — 2024. — URL: https://www.vesti.ru/article/4263555 (дата обращения: 10.01.2025).

8. Soni S.K. Advanced Social Engineering Tactics in Contemporary Cyber Threats / S.K. Soni, P. Singh, A.A. Waoo // Journal of Cybersecurity Research. — 2023. — Vol. 12, № 3. — P. 45–60. DOI: 10.1016/j.jcr.2023.03.005.

9. Manukyan L. Social Engineering Attacks: How to Prevent / L. Manukyan, M. Gevorgyan // JDS. — 2024. — Vol. 6, № 1. — P. 28–35. DOI: 10.33847/2686-8296.6.1_3.

10. Ярославцева К.А. Этические проблемы цифровых технологий / К.А. Ярославцева, Н.В. Пчелинцева, И.В. Чепраков [и др.] // Инженерное обеспечение инновационных технологий в АПК. — Мичуринск-наукоград : Материалы Международной научно-практической конференции, 2022. — С. 255–258.

11. Кильдюшкин Р. За 2024 год в России колоссально увеличилось количество фишинга / Р. Кильдюшкин // Газета.ру. — 2024. — URL: https://www.gazeta.ru/tech/news/2024/12/25/24704798.shtml?updated (дата обращения: 10.01.2025).

12. Dedenok R. Conversation hijacking and how to deal with it / R. Dedenok // Kaspersky blog. — 2023. — URL: https://www.kaspersky.ru/blog/what-is-conversation-hijacking/35187/ (accessed: 10.01.2025).

13. Mash M. Cheat a football club / M. Mash // Kaspersky Blog. — 2019. — URL: https://www.kaspersky.ru/blog/boca-juniors-case/22774/ (accessed: 10.01.2025).

14. Margolin J. Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme / J. Margolin, N. Biase. — 2019. — URL: https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business (accessed: 10.01.2025).

15. Претекстинг // Лаборатория Касперского. — 2022. — URL: https://encyclopedia.kaspersky.ru/glossary/pretexting/ (дата обращения: 10.01.2025).

16. Зотина Е.В. Претекстинг как прием социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему / Е.В. Зотина // Вестник Казанского юридического института МВД России. — 2022. — № 4. — С. 93–99.

17. Солдатова Л. «Ваш родственник попал в беду» – одна из распространенных схем мошенничества / Л. Солдатова // Главное управление МВД России по Самарской области. — 2021. — URL: https://63.mvd.ru/news/item/25415312/ (дата обращения: 10.01.2025).

18. 3 главные схемы телефонных мошенников в 2023 году // Дзен. — 2024. — URL: https://dzen.ru/a/ZDP8tFLNsy5qRNMu (дата обращения: 10.01.2025).

19. МВД России информирует граждан о новой схеме мошенничества // МВД России. — 2021. — URL: https://mvd.ru/news/item/22690363/ (дата обращения: 10.01.2025).

20. О внесении изменений в некоторые акты Правительства Российской Федерации: Постановление Правительства России № 1898: [принят Правительством Российской Федерации 2024-12-26 :2024-12-26]. — Москва : 2024. — 5 с.

21. Федеральный закон № 340-ФЗ: [принят Государственной Думой Российской Федерации 2023-07-11 :одобр. Советом Федерации 2023-07-19]. — Москва : 2023. — 61 с.

22. От фишинга до скаревара: обзор популярных атак социальной инженерии. — 2024. — URL: https://www.securitylab.ru/blog/personal/Neurosinaps/354528.php (дата обращения: 10.01.2025).

23. Tischer M. Users Really Do Plug in USB Drives They Find / M. Tischer, Z. Durumeric, S. Foster [et al.]. — 2016. — URL: https://zakird.com/papers/usb.pdf (accessed: 10.01.2025).

24. Генпрокуратура указала на смену традиционных видов преступности на цифровые // Тасс. — 2025. — URL: https://tass.ru/obschestvo/22831665 (дата обращения: 10.01.2025).

25. Оболенский Д. Рекомендации Артёма Градопольцева: как противостоять социальной инженерии / Д. Оболенский. — 2024. — URL: https://www.sostav.ru/blogs/280059/55151 (дата обращения: 10.01.2025).

26. Автушенко Е. 2023 vs. 2024 – Как менялись методы злоумышленников, и как они будут атаковать в 2025? / Е. Автушенко. — 2024. — URL: https://phishman.ru/blog/2025 (дата обращения: 10.01.2025).

Список литературы на английском языке / References in English

1. Besedina V. Aktual'nye kiberugrozy: III kvartal 2024 goda [Current cyber threats: Q3 2024] / V. Besedina. — 2024. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id1 (accessed: 10.01.2025). [in Russian]

2. Hadnagy C. Social Engineering: The Art of Human Hacking / C. Hadnagy. — Indianapolis : Wiley, 2010. — 384 p.

3. Mitnick K. The Art of Deception: Controlling the Human Element of Security / K. Mitnick. — Hoboken : John Wiley & Sons, 2011. — 368 p.

4. Mitnick K. Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker / K. Mitnick. — New York : Little, Brown and Company, 2011. — 432 p.

5. Hadnagy C. Social Engineering: The Science of Human Hacking / C. Hadnagy. — 2nd ed. — Hoboken : John Wiley & Sons, 2018. — 368 p.

6. IBM X-Force Threat Intelligence Index 2024. — Armonk : IBM, 2024. — URL: https://www.ibm.com/reports/threat-intelligence (accessed: 18.02.2025).

7. V Sbere soobschili, chto uscherb ot moshennikov sostavil 250 mlrd rub. v 2024 godu [Sberbank reported that the damage from fraudsters amounted to 250 billion rubles in 2024] // Vesti — 2024. — URL: https://www.vesti.ru/article/4263555 (accessed: 10.01.2025). [in Russian]

8. Soni S.K. Advanced Social Engineering Tactics in Contemporary Cyber Threats / S.K. Soni, P. Singh, A.A. Waoo // Journal of Cybersecurity Research. — 2023. — Vol. 12, № 3. — P. 45–60. DOI: 10.1016/j.jcr.2023.03.005.

9. Manukyan L. Social Engineering Attacks: How to Prevent / L. Manukyan, M. Gevorgyan // JDS. — 2024. — Vol. 6, № 1. — P. 28–35. DOI: 10.33847/2686-8296.6.1_3.

10. Jaroslavtseva K.A. Eticheskie problemy tsifrovyh tehnologij [The Ethical Challenges of Digital Technology] / K.A. Jaroslavtseva, N.V. Pchelintseva, I.V. Cheprakov [et al.] // Engineering support of innovative technologies in the agro-industrial complex. — Michurinsk-science city : Proceedings of the International Scientific and Practical Conference, 2022. — P. 255–258. [in Russian]

11. Kil'djushkin R. Za 2024 god v Rossii kolossal'no uvelichilos' kolichestvo fishinga [In 2024, the number of phishing increased tremendously in Russia] / R. Kil'djushkin // Gazeta.ru. — 2024. — URL: https://www.gazeta.ru/tech/news/2024/12/25/24704798.shtml?updated (accessed: 10.01.2025). [in Russian]

12. Dedenok R. Conversation hijacking and how to deal with it / R. Dedenok // Kaspersky blog. — 2023. — URL: https://www.kaspersky.ru/blog/what-is-conversation-hijacking/35187/ (accessed: 10.01.2025).

13. Mash M. Cheat a football club / M. Mash // Kaspersky Blog. — 2019. — URL: https://www.kaspersky.ru/blog/boca-juniors-case/22774/ (accessed: 10.01.2025).

14. Margolin J. Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme / J. Margolin, N. Biase. — 2019. — URL: https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business (accessed: 10.01.2025).

15. Preteksting [Pretexting] // Kaspersky Lab. — 2022. — URL: https://encyclopedia.kaspersky.ru/glossary/pretexting/ (accessed: 10.01.2025). [in Russian]

16. Zotina E.V. Preteksting kak priem sotsial'noj inzhenerii, ispol'zuemyj telefonnymi moshennikami: kriminologicheskij vzgljad na problemu [Pretexting as a social engineering technique used by phone scammers: a criminological look at the problem] / E.V. Zotina // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. — 2022. — № 4. — P. 93–99. [in Russian]

17. Soldatova L. «Vash rodstvennik popal v bedu» – odna iz rasprostranennyh shem moshennichestva ['Your relative is in trouble'is one common scam scheme] / L. Soldatova // Main Directorate of the Ministry of Internal Affairs of Russia for the Samara Region. — 2021. — URL: https://63.mvd.ru/news/item/25415312/ (accessed: 10.01.2025). [in Russian]

18. 3 glavnye shemy telefonnyh moshennikov v 2023 godu [3 top phone scam schemes in 2023] // Dzen. — 2024. — URL: https://dzen.ru/a/ZDP8tFLNsy5qRNMu (accessed: 10.01.2025). [in Russian]

19. MVD Rossii informiruet grazhdan o novoj sheme moshennichestva [The Ministry of Internal Affairs of Russia informs citizens about the new fraud scheme] // Russian Ministry of Internal Affairs. — 2021. — URL: https://mvd.ru/news/item/22690363/ (accessed: 10.01.2025). [in Russian]

20. O vnesenii izmenenij v nekotorye akty Pravitel'stva Rossijskoj Federatsii [On Amending Certain Acts of the Government of the Russian Federation] : Resolution of the Government of Russia No 1898: [Adopted by the Government of the Russian Federation 2024-12-26 :2024-12-26]. — Moscow : 2024. — 5 p. [in Russian]

21. Federal'nyj zakon Rossijskoj Federatsii [Federal Law of the Russian Federation] : Federal Law No 340-ФЗ: [Adopted by the State Duma of the Russian Federation 2023-07-11 : approved by Sovetom Federatsii2023-07-19]. — Moscow : 2023. — 61 p. [in Russian]

22. Ot fishinga do skarevara: obzor populjarnyh atak sotsial'noj inzhenerii [From phishing to skarevar: An overview of popular social engineering attacks]. — 2024. — URL: https://www.securitylab.ru/blog/personal/Neurosinaps/354528.php (accessed: 10.01.2025). [in Russian]

23. Tischer M. Users Really Do Plug in USB Drives They Find / M. Tischer, Z. Durumeric, S. Foster [et al.]. — 2016. — URL: https://zakird.com/papers/usb.pdf (accessed: 10.01.2025).

24. Genprokuratura ukazala na smenu traditsionnyh vidov prestupnosti na tsifrovye [The Prosecutor General's Office pointed to the change of traditional types of crime to digital] // Tass. — 2025. — URL: https://tass.ru/obschestvo/22831665 (accessed: 10.01.2025). [in Russian]

25. Obolenskij D. Rekomendatsii Artema Gradopol'tseva: kak protivostojat' sotsial'noj inzhenerii [Artyom Gradopoltsev's recommendations: how to resist social engineering] / D. Obolenskij. — 2024. — URL: https://www.sostav.ru/blogs/280059/55151 (accessed: 10.01.2025). [in Russian]

26. Avtushenko E. 2023 vs. 2024 – Kak menjalis' metody zloumyshlennikov, i kak oni budut atakovat' v 2025? [2023 vs. 2024 – How have the attackers' methods changed, and how will they attack in 2025?] / E. Avtushenko. — 2024. — URL: https://phishman.ru/blog/2025 (accessed: 10.01.2025). [in Russian]