

УДК 331.363

DOI: 10.17586/2310-1172-2026-19-3-98-107

Научная статья

Язык статьи – русский

Организационные аспекты противодействия атакам на основе социальной инженерии

Канд. техн. наук **Гавришев Алексей Андреевич** alexxx.2008@inbox.ru
Московский государственный лингвистический университет
Россия, Москва

В данной работе проведено усовершенствование организационных аспектов противодействия атакам на основе социальной инженерии (СоцИн) для защиты персонала предприятия от них. Показано, что атаки на основе СоцИн выступают одним из наиболее эффективных инструментов кибератак против информационных систем и цифровой инфраструктуры предприятий, используя психологические особенности людей. Подчеркнуто, что в настоящее время человеческий фактор стал играть куда более значимую роль в обеспечении информационной безопасности, чем раньше. Статистические и литературные данные демонстрируют, что атаки на основе СоцИн являются успешными благодаря своей способности обходить традиционные, в основном, технические системы защиты. На основании анализа литературы были описаны отдельные подходы и методики, лежащие в основе таких атак. С учетом полученных данных и литературных источников, предложен обобщенный алгоритм действий злоумышленника при проведении атаки на основе СоцИн. Подчеркнуто, что среди множества мер, применяемых для обеспечения информационной безопасности предприятий любой формы собственности, особое место занимают организационные меры, выступающие в качестве «ядра» общей системы информационной безопасности, связывая между собой правовые и технические меры. Указано, что такие меры, в первую очередь, должны быть направлены на регламентацию функционирования объектов защиты и деятельности должностных лиц в целях обеспечения информационной безопасности посредством выработки определенных правил и требований. Отмечено, что именно организационные меры должны быть первым «барьером» против атак на основе СоцИн. На основе понимания основных механизмов атак на основе СоцИн, с учетом результатов из отдельных работ, предложены практические меры организационного характера для защиты персонала предприятия от них. Практическая значимость представленных результатов заключается в том, что они могут быть полезны руководителям предприятий любой формы собственности и специалистам по информационной безопасности для обеспечения противодействия атакам на основе СоцИн, способствуя совершенствованию организационных аспектов противодействия таким атакам для защиты персонала предприятия от них.

Ключевые слова: персонал, предприятие, социальная инженерия, информационная безопасность, организационные меры.

Ссылка для цитирования:

Гавришев А.А. Организационные аспекты противодействия атакам на основе социальной инженерии // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2026. № 3. С. 98-107.
DOI: 10.17586/2310-1172-2026-19-3-98-107.

Scientific article

Article in Russian

Organizational aspects of countering attacks based on social engineering

Ph.D. **Gavrishev Alexey Andreevich** alexxx.2008@inbox.ru
Moscow State Linguistic University
Russia, Moscow

In this work, the organizational aspects of countering attacks based on social engineering (SE) have been improved to protect the company's personnel from it. It is shown that attacks based on SE are one of the most effective tools for cyber attacks against information systems and digital infrastructure of enterprises, using the psychological characteristics of people. It was emphasized that the human factor has now begun to play a much more significant role in ensuring information security than before. Statistical and literary data demonstrate that attacks based on SE are successful due to their ability to bypass traditional, mostly technical, defense systems. Based on the literature analysis, individual approaches and techniques underlying such attacks have been described. Taking into account the obtained data and literary sources, a simplified algorithm of actions of an attacker during an attack based on SE is proposed. It is emphasized that among the many measures used to ensure the information security of enterprises of any form of ownership, organizational measures occupy a special place, acting as the "core" of the overall information security system, linking legal and technical measures. It is indicated that such measures, first of all, should be aimed at regulating the functioning of security facilities and the activities of officials in order to ensure information security through the development of certain rules and requirements. It is noted that organizational measures should be the first "barrier" against attacks based on SE. Based on an understanding of the basic mechanisms of SE attacks, taking into account the results from individual studies, practical organizational measures are proposed to protect the company's personnel from it. The practical significance of the presented results lies in the fact that they can be useful to managers of enterprises of any form of ownership and information security specialists to counter SE attacks, helping to improve the organizational aspects of countering such attacks to protect enterprise personnel from them.

Keywords: personnel, enterprise, social engineering, information security, organizational measures.

For citation:

Gavrishev A.A. Organizational aspects of countering attacks based on social engineering. *Scientific journal NRU ITMO. Series «Economics and Environmental Management»*. 2026. № 3. P. 98-107. DOI: 10.17586/2310-1172-2026-19-3-98-107.

Введение

По мере того, как цифровая трансформация охватывает всё больше аспектов человеческой жизнедеятельности, возрастает значение информационной безопасности (далее – ИБ) [1]. Современные цифровые технологии, несмотря на их способность повышать эффективность труда и уровень комфорта, одновременно делают физических лиц и предприятия более уязвимыми для киберугроз¹. Одним из наиболее действенных методов осуществления кибератак на информационные системы и цифровую инфраструктуру предприятий признано применение методов социальной инженерии (далее – СоцИн), нацеленных на психологическое воздействие на людей [2-4]. Современные тенденции демонстрируют, что роль человеческого фактора в сфере ИБ стала значительно более существенной по сравнению с ситуацией 20-30 летней давности. В связи с этим, более целенаправленная работа с персоналом, включая его обучение основам ИБ, должно стать одной из первоочередных задач предприятий любой формы собственности [5, 6].

Так, согласно статистическим данным компаний Symantec и IBM Security, доля киберинцидентов, связанных с применением СоцИн, увеличилась с 45% в 2020 году до 61% в 2022 году [2]. По данным Positive Technologies [7], СоцИн используется в 92% кибератак на физических лиц и в 37% кибератак на компании. СоцИн также является основой телефонного мошенничества. Именно поэтому угрозы на основе методов СоцИн нашли свое отражение в текущем законодательстве².

В настоящее время методы СоцИн получили широкое распространение, как в мире, так и в России, поскольку они позволяют успешно обходить традиционные, преимущественно технические, средства кибербезопасности. Используя человеческий фактор, злоумышленники получают преимущество перед технологическими системами защиты, обманывая сотрудников и достигая своих корыстных целей [8, 9]. Это становится возможным, потому что люди – ключевой элемент любой информационной инфраструктуры. Вся система создается для их нужд, они обладают доступом к данным, определенными полномочиями и

¹ Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

² Федеральный закон от 01.04.2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации», Приказ Минздрава России от 03.07.2023 № 340н «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством здравоохранения Российской Федерации»

возможностью совершать операции [5, 8, 9]. При этом способ проникновения в корпоративную сеть для злоумышленника вторичен, важен лишь конечный результат. Сотрудники, взаимодействующие с информационными системами, выступают первой линией обороны, и ее падение практически неизбежно приведет к краху всей системы.

В силу вышеизложенного, в настоящее время одной из наиболее актуальных задач в области обеспечения ИБ предприятий любой формы собственности является анализ методов СоцИн, применяемых для проведения кибератак, и разработка подходов к противодействию данным угрозам с учетом человеческого фактора.

Цель исследования

Цель данного исследования является совершенствование организационных аспектов противодействия атакам на основе социальной инженерии для защиты персонала предприятия от них.

Материалы и методы

Для достижения цели исследования были использованы следующие методы: статистический анализ, описание и обобщение материалов по тематике исследования. Материалами служили данные, полученные из различных источников, в частности: справочная система Консультант Плюс, РИНЦ, КиберЛенинка, поисковая система Yandex и др. Общей методологической основой является системный подход.

Результаты

В настоящее время нет устоявшейся трактовки термина «социальная инженерия» – в различных источниках данный термин трактуется по-разному. Так в ГОСТ Р ИСО/МЭК 27033-3-2014³ под СоцИн понимаются действия по манипулированию людьми в совершении действий или разглашении конфиденциальной информации. В работе О.В. Генне СоцИн трактуется, как совокупность подходов прикладных социальных наук, или прикладной социологии, ориентированной на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним [6]. В работе Е.О. Котляр и соавторов под СоцИн в рамках социологии понимаются методы манипуляции личностью с целью получения необходимой информации [11]. В работе О.В. Зорина атака с использованием методов СоцИн трактуется, как разновидность психологического воздействия, использующего уязвимые места в когнитивных функциях человека [12]. Согласно информации с сайта Kaspersky.ru [13], СоцИн – это метод манипуляции людьми с целью получения их конфиденциальной информации, доступа к ресурсам или других представляющих ценность объектов. В контексте ИБ СоцИн определяется как совокупность уловок с целью сбора информации, подделки или несанкционированного доступа к конфиденциальной информации и наиболее часто является одним из шагов в более сложной схеме мошенничества [6, 11].

Для успешного применения СоцИн в своих корыстных целях, злоумышленники прибегают к широкому спектру тактик и подходов. Часть из них целенаправленно осваивает психологию, гипноз и пр., в то время как другие обладают врожденными способностями. Тем не менее, в любом случае, применение приемов СоцИн подобно творческому процессу, требующему мастерства. Для этого, на начальных этапах, злоумышленнику необходимы средства доступа к объекту своего воздействия. Таковыми могут выступать [4, 6]: телефонные звонки, электронные письма, общение в мессенджерах и социальных сетях, точки доступа к сети, личное взаимодействие и пр. Манипулируя людьми, путем задавания наводящих вопросов или анализируя тембр голоса собеседника, злоумышленники способны выявлять их скрытые потребности, уязвимости и опасения, чтобы незамедлительно использовать эту информацию в своих интересах [1-6].

Основой для успешного использования методов СоцИн в отношении практически любого человека могут являться так называемые «врата сортировки». Это жизненные ориентиры, те вещи, которые наиболее важны для человека [6]. Среди «врат сортировки» обычно выделяются следующие: люди; вещи, действия; ценности; процесс; время; место. Не приводя их подробное описание, представленное в [6], отметим, что обычно каждый человек характеризуется двумя – тремя «вратами сортировки», которые злоумышленник может использовать для достижения своих корыстных целей. Иными словами, «врата сортировки» – это первичный «фильтр», через который нужно «просочиться» злоумышленнику, чтобы втереться в доверие к жертве [6].

После минования указанного «фильтра» злоумышленник может использовать различные присущие людям комплексы и страхи. Выделим некоторые из них [3, 6, 11, 12, 14]:

³ ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Ч. 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления»

1. Доверчивость.
2. Страх.
3. Жадность.

Кроме этого, злоумышленники часто используют следующие психологические приемы, являющиеся частными случаями озвученных выше [8, 12]:

1. Установление временных рамок при выполнении тех или иных действий.
2. Просьба о помощи.
3. Выражение эмпатии собеседнику.
4. Эксплуатация моральных обязательств человека, например, перед обществом, работой и пр.
5. Запугивание человека или использование угроз.
6. Предложение вознаграждения.

Чтобы предотвратить мошеннические действия, связанные с СоцИн, важно понимать тактику, которую используют преступники. Ключевым моментом в создании эффективных мер противодействия является установление формы взаимодействия злоумышленника с жертвой. Такие формы взаимодействия делятся на две основные группы [4, 11]: контактные и бесконтактные формы общения.

Контактная форма подразумевает непосредственное общение злоумышленника и жертвы лицом к лицу или же с использованием технических средств. Бесконтактная форма – не требуется личного или удаленного присутствия злоумышленника при передаче, например, вредоносного программного обеспечения посредством запоминающих устройств.

Классификация известных методов СоцИн по формам общения злоумышленник-жертва приведена на рис. 1 [11].

Контактная форма общения	Бесконтактная форма общения
• Претекстинг; • Фишинг, вишинг, смишинг; • Ты – мне, я – тебе; • Обратная социальная инженерия; • Плечевой серфинг	• Ловля на живца; • Троянский конь; • Взлом эл. почты; • Сбор информации из открытых источников

Рис. 1. Классификация известных методов СоцИн

Опишем особенности методов СоцИн, приведенные на рис. 1 [1-6, 15].

Метод «претекстинг», применяемый при непосредственном контакте злоумышленника и жертвы, основывается на предварительном сборе сведений о ней. Злоумышленник, стремясь выглядеть легитимным в глазах жертвы, выуживает у жертвы более детальные данные.

Метод «фишинг» связан с отправкой поддельных электронных писем от имени известных компаний или людей. В них могут содержаться, например, просьба обновить платежные данные или другую конфиденциальную информацию, предлагается перейти по ссылке на какие-либо сайты и пр. Кроме этого, злоумышленники часто используют запугивающие формулировки или угрозы для побуждения жертвы к действию.

«Вишинг» и «смишинг» являются голосовым и SMS-аналогами «фишинга». При «вишинге» мошенник, представляясь сотрудником банка или технической поддержки, запрашивает конфиденциальные данные под надуманным предлогом. «Смишинг» использует SMS-сообщения для кражи конфиденциальной информации.

Метод «ты – мне, я – тебе» заключается в том, что злоумышленник выдает себя за поставщика какой-либо услуги, позволяющей решить некоторые проблемы жертвы. Связываясь с жертвой по электронной почте или телефону, злоумышленник убеждает ее совершить определенные технические действия, например, установить стороннее программное обеспечение, которое он в дальнейшем сможет использовать для противоправных действий.

Подход «обратная социальная инженерия» заключается в том, что злоумышленник создает ситуацию, в которой жертва сама обращается к нему за помощью, например, в службу технической поддержки.

«Плечевой серфинг» – это непсихологический метод, применяемый злоумышленниками в общественных местах. Так они могут наблюдать за действиями человека, когда тот вводит PIN-код на экране банкомата или пароль на своем ноутбуке.

Метод «ловля «на живца» предполагает использование злоумышленником физических носителей с вирусами (USB-флешки, диски), которые могут специально им оставаться в общественных местах. Любопытство жертвы заставляет ее подключить зараженное устройство к компьютеру, активируя вредоносное программное обеспечение.

Метод «троянский конь» представляет собой вид психологической манипуляции, апеллирующей к страхам и любопытству человека. Жертве отправляется письмо с вложением, которое якобы содержит важную информацию. Открытие жертвой файла приводит к загрузке вредоносной программы, которое злоумышленник может использовать в своих целях.

«Взлом электронной почты и рассылка по контактам» подразумевает получение злоумышленником несанкционированного доступа к электронной почте или социальным сетям жертвы. Он может использовать этот доступ для выманивания денег, рассылки вредоносных ссылок и пр.

«Сбор информации из открытых источников» предполагает использование злоумышленником данных, размещенных жертвой о себе в социальных сетях и других публичных ресурсах. Этот метод больше опирается на исследовательские навыки, чем на психологическое манипулирование, позволяя злоумышленнику получить информацию о личной жизни жертвы.

Злоумышленники часто проявляют определенные черты, соответствующие той роли, которую они играют. Жертвы, в свою очередь, склонны наделять злоумышленника дополнительными положительными качествами, заметив определенные сигналы. Более того, злоумышленник способен навязать своей жертве определенный образ, в рамках которого она начинает испытывать к нему симпатию, что способствует формированию доверия. Людей привлекают те, кто разделяет их интересы, имеет схожий уровень образования и увлечения. Злоумышленники всегда детально анализируют все доступные сведения о своей цели для усиления положительного отношения, прибегая к комплиментам, откровенной лести или используя собственную привлекательность. Помимо этого, злоумышленник может играть на желании людей помогать другим, ведь, оказывая помощь, человек испытывает удовлетворение и чувство собственной силы.

На рис. 2 приведена связь некоторых методов СоцИн, рассмотренных выше, с личными качествами жертвы, на которые они влияют [3].

№	Наивность	Жадность	Доверчивость	Любопытство
1	Фишинг	Троян	Подложные предложения и ссылки	Кви про кво/Qui pro quo
2	Плечевой серфинг		Телефонный фишинг и фрикинг	Дорожное яблоко (ловля «наживца»)
3	Ты – мне, я – тебе		Смишинг	
4	Взлом электронной почты и рассылка по		Обратная социальная инженерия	
5	Претекстинг			

Рис. 2. Связь некоторых методов СоцИн с личными качествами жертвы, на которые они влияют

Для дальнейших рассуждений целесообразно уточнить некоторые термины. Так, несмотря на широкое развитие теории и практики обеспечения ИБ, как в нашей стране, так и за рубежом, однако используемые в отечественном законодательстве, а также в научных публикациях основные термины и определения в области ИБ имеют неоднозначную трактовку, что вызывает значительные трудности в понимании их сущности [16]. Так, в первую очередь, обратим внимание на термин «атака», который имеет в настоящее время широкое употребление. В источнике [17] приводится десяток определений данного термина, контекст которых зависит от области его использования. В частности, в военной сфере под атакой понимается стремительное наступательное движение войск во время боевых действий, в переносном смысле – это решительные действия, активное выступление против кого-либо или чего-либо. В области информационных технологий, под компьютерной атакой, согласно [17], понимается проникновение с помощью специальной программы в вычислительное устройство с целью нарушения его работы, причинения вреда или несанкционированного получения информации. Данное определение созвучно с терминологией, используемой в нормативных правовых актах, например, в федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»⁴. Как видно из приведенных данных, термин «атака» активно используется в области ИБ. В

⁴ Компьютерная атака – это целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия

дальнейшем под термином «атака на основе СоцИн», с учетом приведенных результатов, будем понимать целенаправленные действия по манипулированию людьми в совершении действий, создающих угрозы безопасности конфиденциальной информации.

На основе проведенных данных, с учетом источников [4, 8, 11, 14, 15], может быть предложен обобщенный алгоритм проведения злоумышленником атаки на основе СоцИн, включающий в себя следующие этапы:

1. Подготовка атаки на основе СоцИн: постановка целей атаки на основе СоцИн; подготовка технических средств для проведения атаки на основе СоцИн; подготовка сценария атаки на основе СоцИн; выбор категорий жертв; сбор информации о жертве из открытых и других источников; анализ психологического профиля; выбор целевых триггеров.

2. Воздействие: отправка фишингового сообщения или иное вступление в контакт злоумышленника с жертвой; активация автоматического мышления.

3. Эмоциональный ответ: генерация целевой эмоции; установление доверительных отношений; подавление аналитического контроля.

4. Целевое действие: выполнение требуемого действия; нарушение безопасности объекта атаки.

5. Завершение атаки на основе СоцИн: сокрытие следов; достижение целей; анализ результатов.

Успешность атаки на основе СоцИн на первых этапах зависит от подготовительного этапа. Так современные атаки на основе СоцИн все чаще используют данные из открытых источников для персонализации атак [8, 12]. Глубина персонализации напрямую коррелирует с успешностью атаки. Критическим моментом в данном алгоритме является этап подавления аналитического контроля [14]. Исследования показывают, что в условиях эмоционального возбуждения и когнитивной нагрузки человек склонен принимать решения на основе автоматической обработки информации, даже при наличии соответствующих знаний и навыков безопасного поведения. Автоматическая обработка информации характеризуется высокой скоростью работы и эмоциональной окрашенностью.

Обсуждение

Возвращаясь к вопросу уточнения отдельных терминов и определений в области ИБ, далее обратим внимание на один из самых широко употребляемых терминов в данной области – «информационная безопасность». С учетом направленности статьи, для дальнейших исследований, остановимся на следующем определении – «информационная безопасность организации». Согласно ГОСТ Р 53114-2008⁵ под данным термином понимается состояние защищенности интересов организации в условиях угроз в информационной сфере. При этом возможно ввести другое определение [16]: ИБ организации – это состояние защищенности объектов информационной инфраструктуры организации, при котором обеспечены их устойчивое функционирование, а также обеспечивается конфиденциальность, доступность и целостность информации, обрабатываемой в организации. Для обеспечения конфиденциальности, доступности и целостности информации, обрабатываемой в организации, должны применяться меры, направленные на обеспечение ее безопасности путем принятия правовых, организационных и технических мер.

Среди обозначенных мер особое положение занимают организационные меры, которые по своей сути являются «ядром» в общей системе обеспечения ИБ организации, связывая между собой правовые и технические меры⁶. Организационные меры в системе обеспечения ИБ предприятия играют ключевую роль, определяемую, прежде всего, адекватными и своевременными управленческими решениями руководства. Эти решения должны опираться на действующую нормативно-правовую базу, а также на доступные кадровые и технические ресурсы. При этом значение участия руководства в вопросах обеспечения ИБ сложно переоценить⁷. Именно от его действий зависят планирование мер по защите данных, контроль за их исполнением, распределение ответственности между сотрудниками и пр. Конечной целью организационных мероприятий, инициируемых

таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

⁵ ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

⁶ Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности: учебное пособие. СПб.: НИУ ИТМО, 2014. 173 с., Ишейнов В.Я., Мецатунян М.В. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие. М.: ИНФРА-М, 2024. 256 с.

⁷ Указ Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Постановление Правительства РФ от 15.07.2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

руководством и ответственными лицами, является предотвращение утечки конфиденциальной информации, что, в свою очередь, позволяет минимизировать или полностью исключить риски нанесения ущерба предприятию, который может последовать за подобными инцидентами⁸.

Исходя из сказанного, организационные меры должны быть направлены на регламентацию функционирования объектов защиты и деятельности должностных лиц в целях обеспечения ИБ посредством выработки определенных правил и требований. Таким образом, именно организационные меры, практическая значимость которых в настоящее время неоспорима, должны быть первым «барьером» против атак на основе СоцИн.

На основе понимания основных механизмов атак на основе СоцИн, с учетом результатов из отдельных работ [1-6, 8-15, 18-22], могут быть предложены следующие практические меры организационного характера для защиты персонала предприятия от них:

1. Назначение приказом руководителя сотрудника, ответственного за обеспечение ИБ на предприятии. Рекомендуется, чтобы такой сотрудник был в должности не ниже заместителя руководителя. В отдельных случаях это является обязательным требованием законодательства⁹.

2. Создание на предприятии подразделения, осуществляющего функции по обеспечению ИБ, либо возложение данных функций на существующее подразделение.

3. Разработка алгоритма действий персонала для случаев выявления атак на основе СоцИн. Для обеспечения надежной защиты от подобных угроз следует разработать детальные инструкции для всех сотрудников предприятия. Такие инструкции должны четко регламентировать последовательность действий при выявлении подобных атак. Эту информацию необходимо сделать общедоступной и обеспечить ознакомление с ней всех сотрудников под роспись.

4. Разработка критериев для оценки ценности информации, обрабатываемой в компании, для всех сотрудников. В любой организации, с учетом действующего законодательства, должны существовать правила, определяющие, какие данные являются конфиденциальными. Однако следует учитывать, что даже информация, обычно не считающаяся важной, может быть использована злоумышленниками при проведении атак, включая атаки на основе СоцИн.

5. Минимизация санкционированных руководством отклонений сотрудниками от принятых регламентов и инструкций. При этом ни один работник не должен быть подвергнут взысканию за следование утвержденным правилам.

6. Внедрение процедуры подтверждения личности человека и его полномочий на доступ к запрашиваемым данным. Любая организация должна иметь отлаженную методику проверки личности и ее прав доступа к запрашиваемой информации, особенно в случаях, когда речь идет о доступе к важным данным. Рекомендуется обязать сотрудников осуществлять обратный звонок запрашивающему лицу по номеру телефона из корпоративного справочника.

7. Внедрение практики обязательных пауз при выполнении срочных запросов, связанных с критическими действиями. Это позволяет создать временной буфер для включения аналитического мышления. Рекомендуемая длительность паузы – 15 минут.

8. Обучение сотрудников, включающее в себя:

- проведение регулярных практических занятий с анализом реальных кейсов успешных атак на основе СоцИн;
- проведение психологических тренингов по распознаванию сотрудниками когнитивных искажений и манипуляций;
- развитие навыков критического анализа информации;
- выработку навыков вежливого отказа.

9. Использование скрытых тестовых атак на основе СоцИн. Для этого необходимо создать систему регулярного тестирования устойчивости персонала к атакам на основе СоцИн с использованием реалистичных сценариев. Результаты тестирования должны использоваться для точечного повышения осведомленности в выявленных областях уязвимости.

10. Снижение уровня стресса и улучшение настроения персонала на предприятии так же является важным подходом по противодействию атакам на основе СоцИн. К подобным мероприятиям возможно отнести, например, выполнение совместных оздоровительных упражнений и иных «командообразующих» мероприятий, а так же заботу о психическом и физическом здоровье, а также социальное благополучие.

⁸ Там же.

⁹ Указ Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

11. Внедрение гигиены офисного труда для сотрудников, работающих за персональным компьютером (упражнение для глаз, разминки и пр.)

Заключение

Таким образом, в данной работе проведено усовершенствование организационных аспектов противодействия атакам на основе СоцИн для защиты персонала предприятия от них.

Отмечено, что одним из наиболее действенных методов осуществления кибератак на информационные системы и цифровую инфраструктуру предприятий в настоящее время является применение методов СоцИн, нацеленных на психологическое воздействие на людей [2-4]. Указано, что роль человеческого фактора в сфере ИБ на текущий момент стала значительно более существенной по сравнению с ситуацией 20-30 летней давности. С опорой на статистику и известную литературу [5, 8, 9] показано, что одной из основных причин распространения техник СоцИн является то, что эти методы позволяют злоумышленникам обойти традиционные системы киберзащиты, основанные в большей степени на технологических средствах, за счет использования человеческого фактора. На основе известной литературы [1-6, 15] описаны отдельные подходы и методы, положенные в основу таких атак. В частности, отмечено, что основой для успешного использования методов СоцИн в отношении практически любого человека могут являться так называемые «врата сортировки». Кроме этого, описаны некоторые комплексы и страхи, присущие людям, которые могут быть использованы злоумышленниками. Указано, что важным пунктом для разработки методов предупреждения подобных преступлений является определение формы общения злоумышленника со своей жертвой. Приведена известная классификация методов СоцИн по формам общения злоумышленник-жертва и связь указанных методов с личными качествами жертвы, на которые они влияют. На основе проведенных данных, с учетом источников [4, 8, 11, 14, 15], предложен обобщенный алгоритм проведения злоумышленником атаки на основе СоцИн.

Отмечено, что среди мер, применяемых для обеспечения ИБ предприятий любой формы собственности, особое положение занимают организационные меры, которые по своей сути являются «ядром» в общей системе обеспечения ИБ организации, связывая между собой правовые и технические меры¹⁰. Исходя из сказанного, организационные меры должны быть направлены на регламентацию функционирования объектов защиты и деятельности должностных лиц в целях обеспечения ИБ посредством выработки определенных правил и требований. Таким образом, именно организационные меры должны быть первым «барьером» против атак на основе СоцИн.

На основе понимания основных механизмов атак на основе СоцИн, с учетом результатов из отдельных работ [1-6, 8-15, 18-22], предложены практические меры организационного характера для защиты персонала предприятия от них. Практическая значимость представленных результатов заключается в том, что они могут быть полезны руководителям предприятий любой формы собственности и специалистам по ИБ для обеспечения противодействия атакам на основе СоцИн, способствуя совершенствованию организационных аспектов противодействия таким атакам для защиты персонала предприятия от них.

Литература

1. Сафронова Ж.С., Бразевич Д.С., Бразевич С.С., Василенок В.Л. Социально-экономические детерминанты и риски дистанционной работы в условиях цифровой трансформации // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2026. № 1. С. 116-128. DOI: 10.17586/2310-1172-2026-19-1-116-128.
2. Мельников А.И. Социальная инженерия в цифровой эпохе: анализ методов манипуляции человеческим фактором в целях кибератак // Социально-гуманитарные знания. 2024, № 1. С. 50-54.
3. Михалёва У.А. Претекстинг и способы противодействия ему // Вестник Дагестанского государственного технического университета. Технические науки. 2023. № 2. С. 109-116. DOI: 10.21822/2073-6185-2023-50-2-109-116.
4. Кюннер А.П., Чечулин А.А. Обзор научных работ по социальной инженерии // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2025. № 4. С. 94-106. DOI: 10.61260/2218-130X-2025-4-94-106.
5. Былевский П.Г. Феноменология культуры информационной безопасности. М.: МГЛУ, 2024. 240 с.
6. Генне О.В. Заметки о социальной инженерии // Защита информации. INSIDE. 2006. № 6. С. 16-19.

¹⁰ Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности: учебное пособие. СПб.: НИУ ИТМО, 2014. 173 с., Ишейнов В.Я., Мецатунян М.В. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие. М.: ИНФРА-М, 2024. 256 с.

7. Социальная инженерия [Электронный ресурс]. URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/socialnaya_inzheneriya (дата обращения: 06.07.2026).
8. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.
9. Халилаева Э.И., Маслова М.А., Герасимов В.М. Система противодействия методам социальной инженерии в области информационной безопасности // Вестник УрФО. 2023. № 2. С. 54–61. DOI: 10.14529/secur230205
10. Метельков А.Н. Понятие информационной системы: технические и нормативно-правовые аспекты // Правовая информатика. 2025. № 2. С. 112–118.
11. Котляр Е.О., Мецераков М.О., Бугаев К.Г. Методы социальной инженерии как инструмент хищения конфиденциальных данных пользователей // Охрана, безопасность, связь. 2021. № 6-2. С. 223-230.
12. Зорин В.А. Информационная безопасность и нейробиология социальной инженерии: когнитивные искажения, эмпатия // Информация и безопасность. 2024. № 3. С. 441-448. DOI: 10.36622/1682-7813.2024.27.3.008.
13. Что такое социальная инженерия? [Электронный ресурс]. URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering> (дата обращения: 06.07.2026).
14. Бондаренко Д.А., Бурькова Е.В. Анализ эффективности методов социальной инженерии в фишинге и меры защиты от него // Материалы XII Всерос. конф. «Компьютерная интеграция производства и ИПИ-технологии». Оренбург: ОГУ, 2025. С. 89-93.
15. Заводцев И.В. и др. Методы защиты информационных систем от компьютерных атак, осуществляемых с использованием социальной инженерии (СИ-Атак) // Информационные войны. 2017. №2 (42). С. 82-86.
16. Хорев А.А. Цели и задачи защиты информации // Радиоэлектронные устройства и системы для инфокоммуникационных технологий («РЭУС-ИТ 2025»): Доклады Всероссийской конференции, посвящённой «Дню радио». М.: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова, 2025. С. 275-279.
17. Русский язык как государственный [Электронный ресурс]. URL: <https://rus-gos.spbu.ru/index.php/words/show/1103> (дата обращения: 06.07.2026).
18. Гавришнев А.А. Исследование отдельных вопросов управления кадрами по информационной безопасности в медицинских учреждениях // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2024. № 1. С. 31-41. DOI: 10.17586/2310-1172-2024-17-1-31-41.
19. Гавришнев А.А. Исследование рынка труда в сегменте информационной безопасности для учреждений здравоохранения // Теоретическая и прикладная экономика. 2025. № 1. С. 76-88. DOI: 10.25136/2409-8647.2025.1.71839.
20. Гавришнев А.А. Нормативное регулирование деятельности управленческих кадров по информационной безопасности в сфере здравоохранения // Территория новых возможностей. Вестник Владивостокского государственного университета. 2025. Т. 17. № 3. С. 95-105. DOI: 10.63973/2949-1258/2025-3/095-105
21. Гавришнев А.А. Состояние рынка труда в сегменте управленческих кадров по информационной безопасности учреждений здравоохранения // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2025. № 1. С. 123-133. DOI: 10.17586/2310-1172-2025-18-1-123-133.
22. Гламазда А.В., Шевченко Д.А. Менеджмент компании в условиях санкционного давления и конфронтации // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2026. № 1. С. 61-70. DOI: 10.17586/2310-1172-2026-19-1-61-70.

References

1. Safronova Zh.S., Brazevich D.S., Brazevich S.S., Vasilenok V.L. Social`no-e`konomicheskie determinanty` i riski distancionnoj raboty` v usloviyax cifrovoj transformacii // *Nauchny`j zhurnal NIU ITMO. Seriya «E`konomika i e`kologicheskij menedzhment»*. 2026. № 1. S. 116-128. DOI: 10.17586/2310-1172-2026-19-1-116-128.
2. Mel`nikov A.I. Social`naya inzheneriya v cifrovoj e`poxe: analiz metodov manipulyacii chelovecheskim faktorom v celyax kiberatak // *Social`no-gumanitarny`e znaniya*. 2024, № 1. S. 50-54.
3. Mixalyova U.A. Preteksting i sposoby` protivodejstviya emu // *Vestnik Dagestanskogo gosudarstvennogo texnicheskogo universiteta. Texnicheskie nauki*. 2023. № 2. S. 109-116. DOI: 10.21822/2073-6185-2023-50-2-109-116.
4. Kyuner A.P., Chechulin A.A. Obzor nauchny`x работ po social`noj inzhenerii // *Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby` MChS Rossii*. 2025. № 4. S. 94–106. DOI: 10.61260/2218-130X-2025-4-94-106.
5. By`levskij P.G. Fenomenologiya kul`tury` informacionnoj bezopasnosti. M.: MGLU, 2024. 240 s.
6. Genne O.V. Zametki o social`noj inzhenerii // *Zashhita informacii*. INSIDE. 2006. № 6. S. 16-19.

7. Social'naya inzheneriya [E'lektronny'j resurs]. URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/socialnaya_inzheneriya (data obrashheniya: 06.07.2026).
8. Skabczov N. Audit bezopasnosti informacionny'x sistem. SPb.: Piter, 2018. 272 s.
9. Xalilaeva E'.I., Maslova M.A., Gerasimov V.M. Sistema protivodejstviya metodam social'noj inzhenerii v oblasti informacionnoj bezopasnosti // *Vestnik UrFO*. 2023. № 2. S. 54–61. DOI: 10.14529/secur230205
10. Metel'kov A.N. Ponyatie informacionnoj sistemy': texnicheskie i normativno-pravovy'e aspekty' // *Pravovaya informatika*. 2025. № 2. S. 112–118.
11. Kotlyar E.O., Meshheryakov M.O., Bugaev K.G. Metody' social'noj inzhenerii kak instrument xishheniya konfidential'ny'x dannyx pol'zovatelej // *Oxrana, bezopasnost', svyaz*. 2021. № 6-2. S. 223-230.
12. Zorin V.A. Informacionnaya bezopasnost' i nejrobiologiya social'noj inzhenerii: kognitivny'e iskazheniya, e'mpatiya // *Informaciya i bezopasnost'*. 2024. № 3. S. 441-448. DOI: 10.36622/1682-7813.2024.27.3.008.
13. Chto takoe social'naya inzheneriya? [E'lektronny'j resurs]. URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering> (data obrashheniya: 06.07.2026).
14. Bondarenko D.A., Bur'kova E.V. Analiz e'ffektivnosti metodov social'noj inzhenerii v fishinge i mery' zashhity' ot nego // *Materialy' XII Vseros. konf. «Komp'yuternaya integraciya proizvodstva i IPI-texnologii»*. Orenburg: OGU, 2025. S. 89-93.
15. Zavodcev I.V. i dr. Metody' zashhity' informacionny'x sistem ot komp'yuternyx atak, osushhestvlyayemy'x s ispol'zovaniem social'noj inzhenerii (SI-Atak) // *Informacionny'e vojny'*. 2017. №2 (42). S. 82-86.
16. Xorev A.A. Celi i zadachi zashhity' informacii // *Radioe'lektronny'e ustrojstva i sistemy' dlya infokommunikacionny'x texnologij («RE'US-IT 2025»): Doklady' Vserossijskoj konferencii, posvyashhyonnoj «Dnyu radio»*. M.: Rossijskoe nauchno-texnicheskoe obshhestvo radiotexniki, e'lektroniki i svyazi im. A.S. Popova, 2025. S. 275-279.
17. Russkij yazyk kak gosudarstvenny'j [E'lektronny'j resurs]. URL: <https://rusgos.spbu.ru/index.php/words/show/1103> (data obrashheniya: 06.07.2026).
18. Gavrishev A.A. Issledovanie otdel'ny'x voprosov upravleniya kadrami po informacionnoj bezopasnosti v medicinskix uchrezhdeniyax // *Nauchny'j zhurnal NIU ITMO. Seriya: E'konomika i e'kologicheskij menedzhment*. 2024. № 1. S. 31-41. DOI: 10.17586/2310-1172-2024-17-1-31-41.
19. Gavrishev A.A. Issledovanie ry'nka truda v segmente informacionnoj bezopasnosti dlya uchrezhdenij zdravooxraneniya // *Teoreticheskaya i prikladnaya e'konomika*. 2025. № 1. S. 76-88. DOI: 10.25136/2409-8647.2025.1.71839.
20. Gavrishev A.A. Normativnoe regulirovanie deyatel'nosti upravlencheskix kadrov po informacionnoj bezopasnosti v sfere zdravooxraneniya // *Territoriya novyx vozmozhnostej. Vestnik Vladivostokskogo gosudarstvennogo universiteta*. 2025. T. 17. № 3. S. 95-105. DOI: 10.63973/2949-1258/2025-3/095-105.
21. Gavrishev A.A. Sostoyanie ry'nka truda v segmente upravlencheskix kadrov po informacionnoj bezopasnosti uchrezhdenij zdravooxraneniya // *Nauchny'j zhurnal NIU ITMO. Seriya: E'konomika i e'kologicheskij menedzhment*. 2025. № 1. S. 123-133. DOI: 10.17586/2310-1172-2025-18-1-123-133.
22. Glamazda A.V., Shevchenko D.A. Menedzhment kompanii v usloviyax sankcionnogo davleniya i konfrontacii // *Nauchny'j zhurnal NIU ITMO. Seriya «E'konomika i e'kologicheskij menedzhment»*. 2026. № 1. S. 61-70. DOI: 10.17586/2310-1172-2026-19-1-61-70.

Статья поступила в редакцию 22.04.2026
Принята к публикации 22.04.2026

Received 01.06.2026
Accepted for publication 27.08.2026