МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Разработка модели противодействия деструктивным воздействиям методом социальной инженерии»

Исполнитель _____ Харченко Даниил Андреевич

(подпись) (фамилия, имя, отчество)

Руководитель _____ Лепешкин Олег Михайлович

(подпись) (фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____ Олег Михайлович Лепешкин

(подпись) (фамилия, имя, отчество)

«_____» _____2026 г.

Санкт-Петербург

2026

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»

Заведующий кафедрой

_____ Олег Михайлович Лепешкин

(подпись) (фамилия, имя, отчество)

«_____»_____ 20__ года

Задание

на выпускную квалификационную работу

студенту: Харченко Даниилу Андреевичу

(фамилия, имя, отчество)

1. Тема Разработка модели противодействия деструктивным воздействиям методом социальной инженерии

закреплена приказом ректора Университета от «31» июля 2025 года, № 914-С

2. Срок сдачи законченной работы «26» января 2026 года

3. Исходные данные к выпускной квалификационной работе:

_____

4. Перечень вопросов, подлежащих разработке (краткое содержание работы:

Введение. Актуальность темы, цели и задачи ВКР

Глава 1 Теоритические основы социальной инженерии

(наименование главы)

Глава 2 Анализ состояния защищенности предприятия от угроз социальной инженерии

(наименование главы)

Глава 3 Разработка модели противодействия методом социальной инженерии

(наименование главы)

Заключение. Выводы по работе в целом. Оценка степени решения поставленных задач. Практические рекомендации.

5. Перечень материалов, представляемых к защите:

— Пояснительная записка;

6. Дата выдачи задания: «___» _____ 20___ года

Руководитель выпускной квалификационной работы

Профессор, д.т.н., доцент Лепешкин Олег Михайлович _____

(должность, ученая степень, ученое звание, фамилия, имя, отчество) (подпись)

Задание принял к исполнению «___» _____20___ года

Студент Харченко Даниил Андреевич, ИБ-С20-1 _____

(фамилия, имя, отчество, учебная группа) (подпись)

РЕФЕРАТ

Дипломная работа: ____с., ____рис., _____табл., ____ приложения, _____ источников литературы.

РАЗРАБОТКА модели противодействия деструктивным воздействиям методом социальной инженерии.

Объект исследования - выступает система информационной и организационной безопасности предприятия, включающая технические средства защиты, регламенты, процедуры и персонал, взаимодействующий с информационными ресурсами предприятия.

Предмет исследования - совокупность методов, мер и механизмов противодействия социально-инженерным атакам в рамках корпоративной инфраструктуры предприятия, а также процессы повышения осведомленности и устойчивости сотрудников к деструктивным психологическим воздействиям.

Цель исследования: разработка модели противодействия деструктивным воздействиям методом социальной инженерии, направленной на снижение уязвимости персонала и минимизацию рисков, связанных с компрометацией информации и нарушением технологических процессов.

Задачи исследования:

1. Провести анализ существующих угроз и векторов социальных инженерных атак, характерных для крупных предприятий.
2. Оценить текущий уровень информационной безопасности и осведомленности сотрудников, выявить ключевые уязвимости, связанные с человеческим фактором.
3. Исследовать современные подходы и лучшие практики по противодействию социальной инженерии, включая организационные, технические и образовательные меры.
4. Разработать модель защиты от социально-инженерных атак, включающую превентивные, детектирующие и реагирующие компоненты.

5. Сформировать программу обучения и повышения осведомленности сотрудников, а также рекомендации по внедрению регламентов и технических средств.

Разработана модель противодействия деструктивным воздействиям методом социальной инженерии.

ВВЕДЕНИЕ

В современных условиях стремительного развития информационно-коммуникационных технологий и повсеместной цифровизации хозяйственной деятельности вопросы информационной безопасности приобретают критическое значение. Одним из наиболее распространённых и эффективных способов несанкционированного доступа к информационным ресурсам являются социально-инженерные (социальная инженерия) атаки, направленные на воздействие на поведение и решения сотрудников организации. На промышленных предприятиях потенциальные последствия успешных атак включают утечку конфиденциальной информации, нарушение нормального функционирования технологических процессов, простои и значительные экономические потери. Учитывая высокий человеческий фактор в общей системе информационной безопасности предприятия, разработка модели противодействия деструктивным воздействиям методом социальной инженерии является актуальной задачей для повышения устойчивости предприятия к внешним и внутренним угрозам.

Объектом исследования выступает система информационной и организационной безопасности предприятия, включающая технические средства защиты, регламенты, процедуры и персонал, взаимодействующий с информационными ресурсами предприятия.

Предметом исследования является совокупность методов, мер и механизмов противодействия социально-инженерным атакам в рамках корпоративной инфраструктуры предприятия, а также процессы повышения осведомленности и устойчивости сотрудников к деструктивным психологическим воздействиям.

Целью работы является разработка комплексной модели противодействия деструктивным воздействиям методом социальной инженерии, направленной на снижение уязвимости персонала и минимизацию рисков, связанных с компрометацией информации и нарушением технологических процессов.

Задачи исследования:

1. Провести анализ существующих угроз и векторов социальных инженерных атак, характерных для крупных предприятий.

2. Оценить текущий уровень информационной безопасности и осведомленности сотрудников, выявить ключевые уязвимости, связанные с человеческим фактором.

3. Исследовать современные подходы и лучшие практики по противодействию социальной инженерии, включая организационные, технические и образовательные меры.

4. Разработать комплекс практических рекомендаций.

5. Сформировать программу обучения и повышения осведомленности сотрудников, а также рекомендации по внедрению регламентов и технических средств.

Методы исследования. методы теоретического анализа, методы системного анализа и экспериментальные методы.

Выпускная квалификационная работа состоит из следующих разделов: введения, трех глав, заключения и списка использованной литературы.

В первой главе были изучены теоретические основы социальной инженерии.

Вторая глава была посвящена анализу текущего состояния защищенности предприятия.

На основе этого анализа в третьей главе был разработана модель противодействия социальной инженерии на предприятии.

В заключении представлены итоги исследования и основные выводы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

1.1. Концептуальные основы социальной инженерии: сущность, эволюция, современное состояние

Многомерность понятия "социальная инженерия": терминологический анализ

Термин "социальная инженерия" (СИ) в контексте информационной безопасности не имеет единого общепринятого определения, что отражает сложность и многогранность данного феномена. В наиболее общем виде социальная инженерия может быть определена как система методов и технологий целенаправленного воздействия на сознание и поведение человека с целью получения конфиденциальной информации или несанкционированного доступа к информационным ресурсам [1, с. 34].

Российский исследователь А.Н. Скогорев подчеркивает, что социальная инженерия представляет собой "синтез психологических, социологических и технических знаний, направленный на преодоление человеческого, а не машинного барьера в системах защиты информации" [2, с. 56]. Важным аспектом является разграничение понятий "социальная инженерия" и "социальный инжиниринг". Если последний термин имеет более широкое значение и относится к целенаправленному изменению социальных систем, то в контексте информационной безопасности утвердился именно термин "социальная инженерия" как обозначение метода несанкционированного воздействия.

Ключевыми характеристиками социальной инженерии, отличающими ее от других форм кибератак, являются:

1. Антропоцентричность - человек является одновременно и объектом, и инструментом атаки
2. Не Формализуемость - методы основаны на психологических закономерностях, а не на алгоритмических процедурах
3. Контекстуальность - эффективность методов зависит от конкретной ситуации и особенностей целевой аудитории

4. Адаптивность - методы постоянно эволюционируют в ответ на изменения в системах защиты и повышение осведомленности пользователей

Историческая эволюция социальной инженерии: от психологических операций к киберпреступности

Исторические корни социальной инженерии уходят в глубокую древность. Приемы манипуляции сознанием использовались в военном деле (дезинформация, психологические операции), дипломатии, разведывательной деятельности. Однако как самостоятельное направление в контексте информационной безопасности социальная инженерия сформировалась лишь в конце XX века. Ее эволюцию можно разделить на пять основных этапов:

Первый этап (1970-1980-е годы): предыстория и протоформы
Этот период характеризуется становлением компьютерных технологий и появлением первых хакеров, использовавших простейшие формы социальной инженерии - телефонный фрикинг (phone phreaking). Методы были примитивными и использовались преимущественно из любопытства и исследовательского интереса.

Второй этап (1990-е годы): становление и концептуализация
1990-е годы стали периодом концептуализации социальной инженерии. Ключевую роль сыграла деятельность Кевина Митника, который не только продемонстрировал эффективность социально-инженерных методов, но и систематизировал их в своей книге "Искусство обмана" (2002). Митник показал, что самый надежный пароль можно получить, просто позвонив сотруднику и представившись техподдержкой. Этот период характеризуется переходом от разрозненных приемов к системной методологии.

Третий этап (2000-2008 годы): коммерциализация и массовизация
С развитием интернета и электронной коммерции социальная инженерия превращается в инструмент массового кибермошенничества. Появляются автоматизированные фишинговые рассылки, направленные на похищение финансовых данных. Формируется инфраструктура киберпреступности,

включающая создание и продажу фишинговых конструкторов, баз данных электронных адресов, услуг по организации атак. Социальная инженерия становится бизнесом с четкой экономической моделью.

Четвертый этап (2009-2015 годы): профессионализация и таргетизация Глобальный финансовый кризис 2008-2009 годов и последующая цифровизация бизнес-процессов привели к качественному изменению социальной инженерии. На первый план выходят целевые атаки на бизнес:

1. Spear-phishing - персонализированные фишинговые атаки на конкретных сотрудников
2. Whaling - атаки на высшее руководство компаний
3. BEC (Business Email Compromise) - сложные схемы мошенничества с корпоративной почтой

Этот период характеризуется ростом инвестиций в подготовку атак, использованием профессиональных лингвистов и психологов, активным применением данных из социальных сетей для персонализации атак.

Пятый этап (2016 год - по настоящее время): технологизация и конвергенция

Современный этап развития социальной инженерии характеризуется несколькими ключевыми тенденциями:

1. Конвергенция с технологическими атаками - СИ становится стандартным вектором начального проникновения в сложных целевых атаках (APT)
2. Использование искусственного интеллекта - генерация убедительного контента, анализ поведения жертв, создание deepfake-материалов
3. Эксплуатация новых каналов коммуникации - мессенджеры, социальные сети, корпоративные платформы для совместной работы
4. Глобализация и специализация - формирование международных преступных группировок с четким разделением труда

5. Эксплуатация социально-политического контекста - пандемия COVID-19, удаленная работа, геополитические конфликты [3, с. 89-94]

Принципиальное отличие социальной инженерии от других видов кибератак заключается в том, что она атакует не технические системы, а человеческое сознание. Это определяет ее ключевые особенности:

Сравнительная характеристика технических и социально-инженерных атак:

Критерий	Технические атаки	Социально-инженерные атаки
Объект воздействия	Программное обеспечение, оборудование, сети	Сознание и поведен человека
Методы защиты	Технические средства (брандмауэры, антивирусы, IDS/IPS)	Обучение, организационные мер культура безопасности
Скорость обнаружения	От минут до часов	От дней до месяц (часто обнаруживаются)

Стоимость подготовки	Высокая (требуются технические эксперты)	Относительно низк (особенно для массов атак)
Масштабируемость	Ограничена техническими возможностями	Высокая (особенно п использовании автоматизации)
Адаптивность	Зависит от технических навыков атакующих	Высокая (основана психологической гибкости)

Особенностью социальной инженерии является также ее комплементарность техническим методам. В современных сложных атаках социальная инженерия часто используется для первоначального проникновения, после чего применяются технические методы для расширения доступа и достижения конечной цели.

1.2. Психологические и методологические основы социальной инженерии

1.2.1. Психологические механизмы манипуляции: теоретические модели

Эффективность социальной инженерии основана на фундаментальных закономерностях человеческой психики. Понимание этих механизмов необходимо как для анализа угроз, так и для разработки эффективных контрмер.

Модель шести принципов убеждения Роберта Чалдини Наиболее известной и практически значимой моделью психологических основ

манипуляции является теория шести принципов убеждения, разработанная Робертом Чалдини [4, с. 112-145]:

Принцип взаимного обмена (Reciprocity)

Сущность: Люди чувствуют себя обязанными отвечать услугой на оказанную услугу

Пример в СИ: Социальный инженер сначала предлагает помощь или небольшую услугу, а затем просит о большем одолжении

Эмпирические исследования: Эксперименты показывают, что вероятность выполнения просьбы увеличивается на 15-20% после предварительного оказания услуги

Принцип последовательности и обязательств (Consistency and Commitment)

Сущность: Люди стремятся действовать последовательно со своими предыдущими действиями и заявлениями

Пример в СИ: Получение небольшого начального согласия, которое затем используется для получения более значительных уступок

Механизм: Техника "нога в двери" (foot-in-the-door technique)

Принцип социального доказательства (Social Proof)

Сущность: В неопределенных ситуациях люди ориентируются на поведение других

Пример в СИ: "Все ваши коллеги уже обновили пароли по этой ссылке"

Факторы эффективности: Сходство с референтной группой, количество "доказательств"

Принцип благорасположения (Liking)

Сущность: Люди более охотно соглашаются с теми, кто им нравится

Пример в СИ: Установление личного контакта, поиск общих интересов, комплименты

Компоненты: Физическая привлекательность, сходство, общие интересы, позитивное взаимодействие

Принцип авторитета (Authority)

Сущность: Люди склонны подчиняться лицам, воспринимаемым как авторитетные

Пример в СИ: Имитация руководителя, сотрудника правоохранительных органов, технического специалиста

Символы авторитета: Титулы, униформа, профессиональная лексика, ссылки на экспертизу

Принцип дефицита (Scarcity)

Сущность: Люди более высоко ценят то, что доступно ограниченно

Пример в СИ: "Акция только сегодня", "Ваша учетная запись будет заблокирована через 10 минут"

Психологическая основа: Страх упущенной выгоды (FOMO - Fear Of Missing Out)

Нейропсихологические аспекты манипуляции Современные исследования в области нейронаук позволяют глубже понять механизмы воздействия социальной инженерии на мозг человека:

Эмоциональный захват (Emotional Hijacking) Социальные инженеры часто используют эмоциональные триггеры (страх, жадность, любопытство), которые активируют лимбическую систему мозга, временно подавляя рациональное мышление, связанное с префронтальной корой.

Когнитивная перегрузка (Cognitive Overload) Создание ситуаций, требующих быстрого принятия решений в условиях ограниченного времени, приводит к когнитивной перегрузке, что заставляет мозг использовать эвристики (психологические сокращения) вместо рационального анализа.

Нейропластичность и формирование привычек Повторяющиеся социально-инженерные воздействия могут способствовать

формированию поведенческих паттернов, которые становятся автоматическими и менее подверженными критической оценке [5, с. 67-89].

1.2.2. Когнитивные искажения как основа уязвимости к социальной инженерии

Когнитивные искажения (cognitive biases) - это систематические отклонения в мышлении, которые возникают на основе дисфункциональных убеждений, embedded в когнитивные процессы. В контексте социальной инженерии наиболее значимы следующие искажения:

Искажения, связанные с обработкой информации:

Ошибка подтверждения (Confirmation Bias)

Сущность: Склонность искать, интерпретировать и запоминать информацию, подтверждающую существующие убеждения

Пример в СИ: Сотрудник игнорирует признаки фишинга в письме от "руководства", так как ожидает важных указаний сверху

Экспериментальные данные: Исследования показывают, что люди тратят на 30% больше времени на изучение информации, подтверждающей их гипотезы

Эвристика доступности (Availability Heuristic)

Сущность: Оценка вероятности события по легкости припоминания аналогичных случаев

Пример в СИ: После недавнего инцидента с вишингом сотрудники становятся гипербдительными к телефонным звонкам, но могут пропустить фишинговое письмо

Факторы влияния: Эмоциональная окраска событий, недавность, медийное освещение

Эффект ореола (Halo Effect)

Сущность: Распространение общего впечатления о человеке на оценку его конкретных качеств

Пример в СИ: Авторитетный вид или должность отправителя письма заставляет получателя не критически оценивать содержание

Эксперименты: Исследования показывают, что привлекательные люди оцениваются как более компетентные и заслуживающие доверия

Искажения, связанные с принятием решений: Эффект привязки (Anchoring Effect)

Сущность: Сильное влияние первоначальной информации на последующие суждения

Пример в СИ: Первоначальное упоминание о "критической уязвимости" задает тон всему дальнейшему взаимодействию

Практическое значение: Первое впечатление или первоначальная информация часто определяют весь ход взаимодействия

Иллюзия контроля (Illusion of Control)

Сущность: Переоценка собственной способности влиять на события

Пример в СИ: Сотрудник считает, что может распознать любую попытку обмана, и поэтому не соблюдает формальные процедуры проверки

Факторы усиления: Опыт успешного распознавания атак в прошлом, высокая самооценка

Эффект Даннинга-Крюгера (Dunning-Kruger Effect)

Сущность: Когнитивное искажение, при котором люди с низкой квалификацией делают ошибочные выводы и принимают неудачные решения, но неспособны осознавать свои ошибки в силу низкого уровня своей квалификации

Пример в СИ: Малоопытные сотрудники переоценивают свою способность распознавать социально-инженерные атаки

1.2.3. Модели жизненного цикла социально-инженерных атак

Анализ многочисленных случаев социально-инженерных атак позволяет выделить общую модель жизненного цикла, состоящую из семи основных этапов:

Этап 1: Разведка и сбор информации (Reconnaissance)

Цель: Сбор максимального объема информации о целевой организации и ее сотрудниках

Методы: OSINT (Open Source Intelligence) - анализ сайтов, социальных сетей, пресс-релизов, профессиональных форумов

Инструменты: Специализированное ПО для сбора данных (Maltego, theHarvester), анализ метаданных

Продолжительность: От нескольких дней до нескольких месяцев

Критерий успеха: Получение достаточной информации для персонализации атаки

Этап 2: Выбор цели и разработка сценария (Target Selection and Scenario Development)

Цель: Определение конкретного сотрудника и разработка детального сценария атаки

Критерии выбора цели: Доступ к целевым ресурсам, психологический профиль, поведенческие паттерны

Разработка претекста: Создание правдоподобной легенды, подготовка вспомогательных материалов

Анализ рисков: Оценка вероятности успеха и возможных последствий провала

Этап 3: Установление первоначального контакта (Initial Contact)

Цель: Установление коммуникации с целью без вызова подозрений

Выбор канала: Определение оптимального канала коммуникации (email, телефон, социальные сети)

Техники: Использование принципов благорасположения и социального доказательства

Критерий успеха: Получение позитивного отклика и готовности к дальнейшему взаимодействию

Этап 4: Формирование доверия и построение отношений (Trust Building and Rapport)

Цель: Создание устойчивых доверительных отношений с целью

Методы: Активное слушание, эмпатия, нахождение общих интересов

Техники: Использование принципов взаимного обмена и последовательности

Продолжительность: Зависит от сложности атаки и осторожности цели

Этап 5: Манипуляция и эксплуатация (Manipulation and Exploitation)

Цель: Достижение целевого действия со стороны жертвы

Техники: Использование принципов авторитета, дефицита, социального доказательства

Эскалация: Постепенное увеличение требований от незначительных к критически важным

Преодоление сопротивления: Техники нейтрализации возражений, создание ощущения безвыходности

Этап 6: Достижение цели и завершение взаимодействия (Goal Achievement and Disengagement)

Цель: Получение целевой информации или доступа и безопасное завершение контакта

Методы: Естественное завершение разговора, создание оправданий для прекращения контакта

Минимизация следов: Удаление свидетельств взаимодействия (если возможно)

Этап 7: Постинцидентные действия (Post-Incident Activities)

Анализ успешности: Оценка эффективности использованных методов

Документирование: Фиксация успешных техник и особенностей цели для будущих атак

Монетизация: Использование полученной информации для финансовой выгоды или дальнейшего проникновения [7, с. 123-156]

1.3. Систематизация методов и техник социальной инженерии

1.3.1. Классификационные подходы к методам социальной инженерии

Существует несколько подходов к классификации методов социальной инженерии, каждый из которых имеет свои преимущества и ограничения. Наиболее полной является многомерная классификация, учитывающая канал воздействия, цель атаки, степень персонализации и техническую сложность.

Классификация по каналу воздействия:

1. Электронная почта (фишинг и его разновидности)
2. Массовый фишинг (Spam Phishing): Неперсонализированные рассылки на миллионы адресов
3. Таргетированный фишинг (Spear Phishing): Персонализированные атаки на конкретных сотрудников
4. Китобойный промысел (Whaling): Атаки на высшее руководство организаций
5. BEC (Business Email Compromise): Сложные схемы мошенничества с корпоративной почтой
6. Клон-фишинг (Clone Phishing): Создание точной копии легитимного письма с заменой вложений или ссылок

Статистика: По данным APWG (Anti-Phishing Working Group), в 2023 году было зафиксировано более 1,2 миллиона фишинговых атак, при этом 65% из них были целевыми [8, с. 34].

Телефонные атаки (вишинг):

1. Классический вишинг: Звонки с целью получения конфиденциальной информации
2. Технический вишинг: Звонки под видом технической поддержки
3. Имитационный вишинг: Использование технологий подмены номера (спуфинг) и синтеза речи
4. Обратный вишинг: Побуждение жертвы перезвонить на контролируемый злоумышленником номер

Особенности: Высокая эффективность за счет непосредственного контакта и возможности мгновенной адаптации к реакции жертвы.

SMS и мессенджеры (смишинг):

1. Мессенджер-фишинг: Атаки через WhatsApp, Telegram, Viber, MAX
2. QR-фишинг: Использование QR-кодов для скрытия фишинговых ссылок

Тренды: Рост популярности в связи с высокой открываемостью SMS (до 98%) и доверием к сообщениям в мессенджерах.

Социальные сети:

1. Квид про-профилинг: Создание фальшивых профилей для установления доверительных отношений
2. Социальный фишинг: Использование информации из социальных сетей для персонализации атак
3. Фарминг репутации: Создание положительного имиджа для последующего использования в атаках

Особенности: Длительный характер атак (от нескольких недель до месяцев), высокая степень персонализации.

Физические методы

1. Претекстинг (Pretexting): Создание вымышленного сценария для получения информации
2. Тэйлгейтинг (Tailgating): Проникновение в охраняемые зоны вслед за авторизованным лицом
3. Байтинг (Baiting): Использование физических приманок (флешки, документы)
4. Сбор мусора (Dumpster Diving): Поиск конфиденциальной информации в отходах
5. Наблюдение (Shoulder Surfing): Визуальное наблюдение за вводом паролей и другой информации

Эффективность: Несмотря на кажущуюся простоту, физические методы остаются чрезвычайно эффективными, особенно против организаций с сильной технической, но слабой физической защитой.

1.3.2. Технические аспекты реализации социально-инженерных атак

Современные социально-инженерные атки часто используют сложные технические средства для повышения эффективности:

Технологии создания фишинговых ресурсов:

Фишинговые конструкторы: ПО для автоматического создания фишинговых страниц (Social-Engineer Toolkit, GoPhish)

Клонирование сайтов: Технологии создания точных копий легитимных сайтов

Обфускация кода: Методы скрытия фишингового кода от систем защиты

DNS-спуфинг: Техники подмены DNS-записей для перенаправления на фишинговые сайты

Средства автоматизации и масштабирования:

Сбор и обработка данных: Автоматизированный сбор информации из открытых источников

Генерация контента: Использование языковых моделей (GPT) для создания убедительных текстов

Управление кампаниями: Платформы для координации масштабных фишинговых кампаний

Анализ эффективности: Системы отслеживания открытий писем, переходов по ссылкам, ввода данных

Технологии усиления убедительности:

Спуфинг идентификаторов: Подмена email-адресов, телефонных номеров, IP-адресов

Синтез и распознавание речи: Для создания реалистичных голосовых сообщений и анализа эмоций

Deepfake-технологии: Создание поддельных аудио- и видеоматериалов

Социальные боты: Автоматизированные аккаунты в социальных сетях для создания иллюзии популярности или поддержки [9, с. 178-201]

1.3.3. Комплексные и гибридные атаки

Современные социально-инженерные атаки все реже используются изолированно. Чаще они являются частью сложных многоэтапных операций:

Модель конвергентной атаки:

Этап 1: Социальная инженерия - получение первоначального доступа

Этап 2: Техническая эксплуатация - установка вредоносного ПО, повышение привилегий

Этап 3: Движение по сети - исследование инфраструктуры, поиск целевых данных

Этап 4: Достижение цели - хищение данных, саботаж, шантаж

Этап 5: Сокрытие следов - удаление логов, установка backdoor-ов

Примеры сложных атак:

APT-кампании: Длительные целевые атаки, сочетающие социальную инженерию с продвинутыми техническими методами

Цепочки поставок (Supply Chain): Атаки через партнеров и поставщиков, где социальная инженерия используется для компрометации менее защищенных звеньев цепи

Атаки на удаленных сотрудников: Эксплуатация уязвимостей домашних сетей и личных устройств через социальную инженерию

1.4. Цели, мотивация и экономика социально-инженерных атак

1.4.1. Многоуровневая система целей социальной инженерии

Цели социально-инженерных атак могут быть классифицированы по нескольким уровням:

Тактические цели (непосредственный результат атаки):

Получение учетных данных: Логины, пароли, PIN-коды, токены доступа

Установка вредоносного ПО: Трояны, клавиатурные шпионы, ransomware

Финансовые операции: Переводы денежных средств, оформление кредитов

Раскрытие информации: Коммерческая тайна, персональные данные, служебная информация

Оперативные цели (промежуточные результаты):

Доступ к системам: Корпоративные сети, облачные сервисы, базы данных

Повышение привилегий: Получение прав администратора, доступа к критическим системам

Создание точек постоянного доступа: Установка backdoor-ов, создание скрытых учетных записей

Разведка инфраструктуры: Составление карты сети, инвентаризация систем и данных

Стратегические цели (конечные результаты):

Финансовая выгода: Прямое обогащение через хищение средств или продажу информации

Конкурентное преимущество: Получение коммерческой тайны конкурентов

Операционный ущерб: Остановка производства, нарушение бизнес-процессов

Репутационный ущерб: Подрыв доверия клиентов, партнеров, инвесторов

Политическое влияние: Вмешательство в политические процессы, влияние на общественное мнение [10, с. 89-112]

1.4.2. Мотивационная структура субъектов социальной инженерии

Мотивация лиц, осуществляющих социально-инженерные атаки, может быть классифицирована следующим образом:

Криминальная мотивация:

Финансовая: Прямое получение денежных средств (76% атак по данным Verizon DBIR 2023)

Экономическая: Получение коммерческой информации для конкурентной борьбы

Профессиональная: Социальная инженерия как основной источник дохода

Идеологическая мотивация:

Политическая: Влияние на политические процессы, поддержка определенных сил

Идеологическая: Продвижение определенных идей, ценностей, взглядов

Активистская: Действия в рамках хактивизма, киберпротестов

Психологическая мотивация:

Самовыражение: Демонстрация своих способностей, получение признания

Любопытство: Исследовательский интерес, желание проверить границы возможного

Месть: Действия против бывших работодателей, коллег, организаций

Власть и контроль: Удовлетворение от управления поведением других людей

Государственная мотивация:

Разведывательная деятельность: Сбор разведданных в интересах государства

Контрразведывательная деятельность: Противодействие разведке противника

Операции информационного воздействия: Влияние на общественное мнение других стран [11, с. 134-156]

1.4.3. Экономическая модель социально-инженерных атак

Социальная инженерия как вид киберпреступности имеет четкую экономическую модель:

Структура затрат:

Подготовительные затраты: Сбор информации, разработка сценариев, создание инструментов

Операционные затраты: Проведение атак, поддержка инфраструктуры, оплата услуг посредников

Рисковые затраты: Страхование от провала, юридические издержки, затраты на безопасность

Структура доходов:

Прямые доходы: Хищение денежных средств, выкуп за расшифровку данных

Косвенные доходы: Продажа украденных данных, учетных записей, доступа к системам

Производные доходы: Использование полученной информации для других видов преступной деятельности

Показатели эффективности:

ROI (Return on Investment): Отношение полученного дохода к затратам на атаку

Уровень успешности: Процент успешных атак от общего числа попыток

Время до обнаружения: Среднее время от момента атаки до ее обнаружения

Стоимость инцидента: Средний ущерб от успешной атаки для организации-жертвы

Рыночные тенденции:

Специализация: Формирование рынка специализированных услуг (сбор информации, создание фишинговых страниц, проведение атак)

Стандартизация: Появление стандартных пакетов услуг и ценовых моделей

Глобализация: Создание международных преступных сетей с разделением труда по странам и регионам

Технологизация: Инвестиции в разработку и совершенствование инструментов для автоматизации атак [12, с. 201-223]

1.5. Специфика социальной инженерии в контексте промышленных предприятий

1.5.1. Промышленные предприятия как целевые объекты: анализ уязвимостей

Промышленные предприятия, особенно относящиеся к критической информационной инфраструктуре (КИИ), представляют особый интерес для злоумышленников по нескольким причинам:

Факторы привлекательности:

Высокая стоимость простоя: Минута простоя крупного промышленного предприятия может стоить десятки тысяч долларов

Критичность последствий: Успешная атака может привести к экологическим катастрофам, человеческим жертвам, масштабным экономическим потерям

Ценность активов: Промышленные секреты, технологии, ноу-хау представляют высокую коммерческую ценность

Сложность защиты: Сочетание IT и OT (Operational Technology) систем создает дополнительные уязвимости

Особенности организационной структуры:

Иерархичность: Четкая иерархия облегчает имитацию руководства

Разделение ответственности: Размытость зон ответственности между IT и производственными подразделениями

Культурные особенности: Приоритет производственных показателей над вопросами безопасности

Кадровый состав: Разнообразие уровня цифровой грамотности среди сотрудников

1.5.2. Профили уязвимых групп персонала промышленных предприятий

Анализ успешных атак на промышленные предприятия позволяет выделить следующие уязвимые группы персонала:

Технический персонал и инженеры АСУ ТП:

Уровень доступа: Высокий (критические производственные системы)

Психологический профиль: Технически ориентированные, доверяющие "техническим" аргументам

Типичные сценарии атак: Фишинг под видом вендоров оборудования, запросы на дистанционное обслуживание, уведомления о "критических обновлениях"

Статистика: По данным исследования Positive Technologies, 42% успешных атак на промышленные предприятия начинаются с компрометации технического персонала [13, с. 45]

Руководящий состав:

Уровень доступа: Максимальный (стратегическая информация, финансовые полномочия)

Психологический профиль: Высокая занятость, привычка делегировать, доверие к формальным процедурам

Типичные сценарии атак: Whaling, BEC, имитация запросов от вышестоящих органов

Эффективность: Уровень успешности атак на руководство в 3-4 раза выше, чем на рядовых сотрудников

Финансово-экономические службы:

Уровень доступа: Ключевой (финансовые операции, коммерческая информация)

Психологический профиль: Ориентированы на выполнение указаний, работа в условиях регламентов

Типичные сценарии атак: BEC, вишинг под видом банков, поддельные платежные документы

Ущерб: Средний размер ущерба от успешной BEC-атаки на промышленное предприятие составляет $1.5-2 млн.

Службы безопасности и режимные подразделения:

Уровень доступа: Критический (физическая безопасность, доступ на территорию)

Психологический профиль: Ориентированы на формальные процедуры, могут недостаточно критически оценивать нестандартные ситуации

Типичные сценарии атак: Претекстинг, имитация проверок, создание искусственных инцидентов для отвлечения внимания

1.5.3. Особенности социально-инженерных атак на промышленные предприятия

Анализ реальных инцидентов позволяет выделить специфические особенности социально-инженерных атак на промышленный сектор:

Использование производственного контекста:

Эксплуатация специфической терминологии: Использование профессионального жаргона для создания доверия

Маскировка под техническую документацию: Фишинговые письма в виде технических спецификаций, чертежей, инструкций

Имитация аварийных ситуаций: Создание ощущения срочности на основе производственных инцидентов

Использование цепочек поставок: Атаки через партнеров и подрядчиков

Долгосрочные и многоэтапные операции:

Разведка может длиться месяцами: Детальное изучение производственных процессов, графика работы, персонала

Постепенное проникновение: От периферийных систем к критически важным

Создание постоянного присутствия: Установка backdoor-ов для долгосрочного доступа

Синхронизация с производственным циклом: Проведение атак в наиболее уязвимые моменты (плановые остановки, ввод нового оборудования)

Комбинация социальной инженерии с другими методами:

Интеграция с техническими атаками на ОТ: Социальная инженерия для получения доступа, затем техническая атака на промышленные системы

Использование физических методов: Сочетание кибератак с физическим проникновением

Эксплуатация человеческого фактора на всех уровнях: От рядовых операторов до высшего руководства [14, с. 167-189]

1.6. Выводы по первой главе

Проведенный в первой главе комплексный теоретический анализ социальной инженерии как угрозы информационной безопасности позволяет сформулировать следующие основные выводы:

Социальная инженерия представляет собой сложный многоаспектный феномен, который эволюционировал от простых приемов манипуляции до высокотехнологичной системы киберпреступности. Ее историческое развитие демонстрирует постоянную адаптацию к изменениям в технологической среде и системах защиты, что делает ее одной из наиболее устойчивых и опасных угроз информационной безопасности.

Психологическая основа социальной инженерии базируется на фундаментальных законах человеческой психики - принципах убеждения по Чалдини и когнитивных искажениях. Понимание этих механизмов является ключевым как для анализа угроз, так и для разработки эффективных контрмер. Особую опасность представляет способность социальной инженерии обходить рациональное мышление, воздействуя непосредственно на эмоциональные центры мозга.

Методология социально-инженерных атак характеризуется высокой степенью системности и адаптивности. Модель жизненного цикла, включающая семь этапов от разведки до постинцидентных действий, демонстрирует профессиональный подход современных злоумышленников. Классификация методов по каналам воздействия показывает разнообразие техник, каждая из которых требует специфических контрмер.

Цели и мотивация социально-инженерных атак образуют сложную многоуровневую систему, включающую тактические, оперативные и стратегические цели. Экономическая модель социальной инженерии как вида

киберпреступности демонстрирует высокую рентабельность и способствует постоянному совершенствованию методов и инструментов атак.

Промышленные предприятия представляют собой особо привлекательные цели для социально-инженерных атак в силу высокой стоимости простоя, критичности последствий и сложности защиты. Специфика этих предприятий определяет уникальные векторы атак, использование производственного контекста и комбинацию социальной инженерии с другими методами воздействия.

Теоретический анализ выявил системный характер угрозы социальной инженерии, что требует адекватного системного подхода к противодействию. Частичные и разрозненные меры не могут обеспечить эффективную защиту от социально-инженерных атак, что обосновывает необходимость разработки комплексных моделей противодействия, учитывающих все аспекты данной угрозы.

ГЛАВА 2. АНАЛИЗ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ПРЕДПРИЯТИЯ ОТ УГРОЗ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

На основе теоретических основ социальной инженерии (СИ), изложенных в первой главе, вторая глава посвящена практическому анализу уровня защищенности конкретного промышленного предприятия - АО «Кольская горно-металлургическая компания» , являющегося субъектом критической информационной инфраструктуры (КИИ). Целью главы является проведение комплексной оценки уязвимости предприятия к социально-инженерным атакам с выявлением направлений для совершенствования системы защиты. Для достижения цели последовательно решаются задачи: 1) характеристика объекта исследования как субъекта КИИ; 2) разработка методики оценки; 3) анализ состояния защищенности по организационному, техническому и кадровому направлениям с использованием данных эмпирического исследования; 4) моделирование и оценка рисков ключевых сценариев атак; 5) формулировка свободных выводов. Результаты анализа служат основой для проектирования модели противодействия в третьей главе.

2.1. Общая характеристика объекта исследования: АО «Кольская ГМК»

2.1.1. Организационно-технологический профиль и статус субъекта КИИ

Акционерное общество «Кольская горно-металлургическая компания» (производственная площадка в г. Мончегорск) является стратегическим активом ПАО «ГМК «Норильский никель» и осуществляет завершающие, стадии производства никеля, кобальта и сопутствующих металлов. Согласно Постановлению Правительства РФ, предприятия цветной металлургии, обеспечивающие национальную безопасность и экономическую устойчивость, могут быть отнесены к субъектам КИИ [15]. Информационные системы, используемые для управления непрерывными и опасными производственными процессами (электролиз, плавка, химическая переработка) на данной площадке, в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности

критической информационной инфраструктуры Российской Федерации» признаны критически важными [15]. Это накладывает на предприятие обязательства по соблюдению установленных ФСТЭК России требований к обеспечению их безопасности, включая защиту от компьютерных атак, к которым правомерно относятся и атаки методами социальной инженерии, направленные на персонал, управляющий этими системами [13, 17].

2.1.2. Детализация информационной инфраструктуры и ключевых информационных активов

Информационная среда предприятия представляет собой двухконтурную архитектуру, типичную для современного промышленного объекта КИИ.

Контур информационных технологий (IT-инфраструктура):

1. Корпоративная сеть: Интегрирована в сеть холдинга, включает сегменты для административного, инженерного и технологического персонала. Ключевые сервисы: корпоративная электронная почта, системы электронного документооборота и коллаборации (Microsoft 365), ERP-система (SAP), системы кадрового и финансового учёта.

2. Ключевые информационные активы IT-контура:

a. Объекты повышенной защищаемости (по ФЗ-187): Базы данных, содержащие коммерческую тайну (технологические регламенты, методики рафинирования), персональные данные сотрудников, оперативно-коммерческую информацию (планы отгрузки, себестоимость), проектную документацию.

Контур операционных технологий (OT-инфраструктура / АСУ ТП):

1. Архитектура АСУ ТП: Многоуровневая система, включающая датчики, программируемые логические контроллеры (ПЛК, например, Siemens SIMATIC), человеко-машинные интерфейсы (АРМы) и серверы SCADA/DCS (Siemens WinCC, Wonderware). Сети АСУ ТП должны быть выделены в соответствии с требованиями к КИИ.

2. Критичные активы OT-контура (непосредственно объекты КИИ):

2.1. Программное обеспечение и конфигурации АСУ ТП, управляющие технологическими процессами.

2.2. Реальные технологические данные (телеметрия), являющиеся основой для управления и ноу-хау.

2.3. Системы промышленной безопасности, интегрированные с АСУ ТП.

Точки интеграции и уязвимости: Наиболее рискованными с точки зрения социальной инженерии являются сотрудники и системы, обеспечивающие обмен данными между IT и OT-контурами, так как они создают потенциальные пути преодоления изоляции сетей КИИ [19, с. 45].

2.1.3. Организационная структура и категоризация персонала по профилю уязвимости

Персонал, имеющий доступ к объектам КИИ или управляющий ими, представляет собой особо значимые целевые группы:

1. Менеджмент (руководство): Обладают широкими полномочиями и доступом к стратегической информации. Цель для whaling и BEC-атак.

2. Инженерно-технический персонал: Непосредственно работают с системами КИИ (АСУ ТП, КИПиА). Высокий риск стать жертвой целевого фишинга под видом вендоров.

3. Рабочие цехов: Управляют технологическими процессами в реальном времени. Уязвимы для вишинга и претекстинга, что может привести к прямым операционным воздействиям.

4. ИТ-специалисты и администраторы: Обеспечивают функционирование инфраструктуры. Цель для атак с целью получения привилегированного доступа.

2.2. Методика оценки уязвимости предприятия к социальной инженерии

2.2.1. Критерии и комплекс показателей оценки защищенности субъекта КИИ

Оценка проводилась на основе системы критериев, учитывающих как требования регуляторов в области КИИ, так и лучшие практики [13, 14, 18].

1. Организационно-управленческие критерии: Соответствие политик и регламентов требованиям ФСТЭК к КИИ; известность и выполнимость процедур для персонала; формализация процессов управления доступом к объектам КИИ.

2. Технические критерии: Наличие и эффективность средств защиты, соответствующих приказу ФСТЭК №31 [17]; сегментация сетей КИИ; использование MFA для доступа к критичным системам; защита каналов коммуникаций.

3. Кадровые критерии (человеческий фактор): Уровень осведомлённости персонала, работающего с КИИ; наличие и качество обязательного обучения по требованиям ФСТЭК; сформированность поведенческих паттернов; функционирование системы оповещения об инцидентах.

2.2.2. Матрица оценки рисков для субъекта КИИ Использовалась матрица рисков, где вероятность (P) оценивалась с учётом данных опроса и отраслевой статистики, а воздействие (I) - с учётом критериев критичности, установленных для объектов КИИ [15].

2.3. Анализ текущего состояния защищенности АО «Кольская ГМК» по ключевым направлениям

2.3.1. Оценка соответствия организационно-управленческих мер требованиям к КИИ

Как субъект КИИ, предприятие обязано иметь комплекс организационных документов. Результаты опроса указывают на необходимость совершенствования коммуникации и доведения регламентов: 42% респондентов (21 человек из 50) точно знают внутренний порядок сообщения о подозрительных событиях. Для субъекта КИИ, где оперативность реагирования на инцидент критична, существует потенциал для повышения этого показателя.

Кроме того, высокий уровень сдерживающих факторов для сообщений (72% боятся сообщать о подозрительных инцидентах) указывает на необходимость развития доверительной и не карательной культуры безопасности, что является важным элементом эффективной системы защиты КИИ.

2.3.2. Оценка технических мер защиты в контексте требований к КИИ

Предприятие реализует набор технических мер, предписанных для защиты КИИ (сегментация, средства обнаружения вторжений). Дополнительный фокус может быть направлен на решения, усиливающие защиту именно от социальной инженерии:

1. Защита от целевого фишинга: Повышение эффективности фильтрации персонализированных атак, использующих контекст КИИ.
2. Многофакторная аутентификация (MFA): Расширение применения MFA для доступа к системам управления КИИ в качестве дополнительного барьера.
3. Мониторинг поведения: Развитие систем для выявления аномалий в действиях пользователей после потенциальной компрометации учетных данных.

2.3.3. Анализ кадрового аспекта защищенности: интерпретация результатов анкетирования

Данные анонимного опроса сотрудников ключевых подразделений (инженерно-технический персонал, рабочие цехов, менеджмент) позволяют провести многофакторную оценку и выявить четкие векторы для развития системы безопасности.

1. Базовый уровень информированности и потенциал роста практических компетенций:

1. 78% сотрудников знакомы с термином «фишинг».
2. Интерпретация: На предприятии ведется работа по информированию персонала об основных киберугрозах. Этот показатель является прочной основой для перехода к следующему этапу — формированию устойчивых навыков.

3. 54% смогли верно идентифицировать фишинг в тестовом примере.

Интерпретация: Наблюдается разрыв между теоретическим знанием и практическим умением. Это указывает на то, что значительная часть персонала (54%) уже способна применять знания на практике. Стратегической задачей является повышение этого процента через внедрение интерактивных, практико-ориентированных форматов обучения (разбор кейсов, симуляции), которые помогут остальным 46% сотрудников преодолеть этот разрыв.

2. Потенциал для систематизации и расширения образовательных программ:

По полученным данным 66% сотрудников не проходили специализированного обучения по противодействию СИ.

Интерпретация: Данный показатель четко определяет целевую аудиторию и масштаб задачи. Важно сделать обучение регулярным и обязательным элементом корпоративной культуры, что полностью согласуется с требованиями ФСТЭК к подготовке персонала КИИ [13].

3. Выявление конкретных поведенческих паттернов, требующих коррекции через целевой тренинг:

46% считают допустимым открыть срочное вложение от «коллеги» без проверки.

Интерпретация: Данный результат служит точной мишенью для поведенческого тренинга. Программы должны учить сотрудников алгоритму «паузы и верификации» даже в условиях стресса и цейтнота, характерных для производственного предприятия.

4. Области для укрепления организационных процедур и культуры личной ответственности:

Только 34% сотрудников считают, что их действия могут привести к серьезному инциденту.

Интерпретация: Данный результат отражает восприятие информационной безопасности как прерогативы специализированных подразделений (ИТ, СБ).

Задачей является разработка коммуникационных и обучающих программ, которые наглядно, на примерах из промышленного контекста, покажут прямую причинно-следственную связь между действием рядового инженера или оператора и потенциальными последствиями для технологического процесса, тем самым формируя понимание личной ответственности:

Только 42% точно знают регламент сообщения о подозрительных событиях.

Интерпретация: Показатель демонстрирует необходимость в упрощении, стандартизации и активном продвижении процедуры сообщения об инциденте. Регламент может существовать, но он либо сложен, либо плохо анонсирован. Цель — сделать его таким же известным, как правила охраны труда.

5. Критический анализ механизма обратной связи и корпоративной культуры безопасности.

74% не знают, куда сообщить об инциденте.

Интерпретация: Это показатель технического разрыва в коммуникации. Система реагирования существует, но её «входная точка» не очевидна для большинства сотрудников.

72% боятся сообщать информацию о подозрительных инцидентах.

Интерпретация: Это наиболее значимая находка опроса, раскрывающая глубинную проблему организационной культуры. Страх сообщать указывает на возможное восприятие службы безопасности как карательного органа, а не как партнера в обеспечении безопасности. Без решения этой проблемы любые технические и процедурные меры будут неэффективны, так как система лишится критически важного источника информации об угрозах. Необходимо строить доверительные, не карательные механизмы обратной связи, с элементами анонимности, поощрения бдительности и разъяснения, что сообщение о потенциальной угрозе — это проявление ответственности, а не ошибка.

6. Коррекция восприятия профиля угроз для повышения всеобщей бдительности:

58% полагают, что главной целью являются только руководители высшего звена.

Интерпретация: Это распространенное заблуждение создает «слепую зону», снижая бдительность у инженерного и технического персонала, который на самом деле является первоочередной мишенью для получения доступа к системам. Образовательные материалы должны наглядно разъяснять тактику злоумышленников, показывая, что атака на рядового специалиста — это стандартный, а не исключительный сценарий.

Таблица 2.1 - Результаты анонимного анкетирования сотрудников АО «Кольская ГМК» (50 человек) и направления для развития

№	Параметр оценки	результат	Направление для совершенствования
1	Знание термина «фишинг»	78% (39 чел.)	Необходимо перевести знания в навыки.
2	Умение идентифицировать фишинг на практике	54% (27 чел.)	Внедрение практико-ориентированных тренингов и симуляций.
3	Прохождение специализированного обучения по СИ	34% (17 чел.)	Разработка и внедрение обязательной регулярной программы обучения для 66% сотрудников.
4	Готовность открыть срочное вложение в сообщении	46% (23 чел.)	Это поведенческая уязвимость. Нужны тренинги по противодействию

	без проверки		манипуляциям на основе срочности и авторитета.
5	Понимание личной ответственности за инциденты ИБ	34% (17 чел.)	Необходимо внедрить программы, демонстрирующие роль каждого в защите КИИ.
6	Знание регламента сообщения об инциденте	42% (21 чел.)	Важно улучшение коммуникации. Упрощение и популяризация процедуры сообщения об инциденте.
7	Отсутствие страха сообщать об инциденте	28% (14 чел.)	Создание доверительной среды. Внедрение некарательной политики и поощрение бдительности.
8	Восприятие себя как цели атаки	42% (21 чел.)	Нужно внедрение разбора реальных кейсов атак на инженерный персонал.

Итог по анализу опроса: Результаты указывают на необходимость конкретных шагов по эволюции системы безопасности. Основной вектор — переход от разрозненных информационных активностей к системной программе управления человеческим фактором, включающей цикличное обучение, тренировку поведенческих навыков и целенаправленное формирование позитивной культуры безопасности с доверительной обратной связью.

2.4. Моделирование ключевых сценариев атак и оценка рисков для субъекта КИИ

Для оценки рисков была применена адаптированная методика качественного анализа рисков на основе рекомендаций ФСТЭК России и стандарта ГОСТ Р ИСО/МЭК 27005. Оценка проводилась в три этапа:

1. Определение вероятности (P). Вероятность успешной реализации сценария оценивалась по 5-балльной шкале на основе комбинации двух ключевых факторов, выявленных в ходе анкетирования:

- Фактор F1: Уровень практической подготовленности персонала. Базовое значение определялось как (100% - % сотрудников, верно идентифицировавших фишинг). То есть, чем меньше сотрудников распознают угрозу, тем выше базовая вероятность. Для сценариев, не связанных с фишингом (вишинг), использовался обобщенный показатель недостатка обучения (66% не обучались).
- Фактор F2: Наличие специфичного опасного поведенческого паттерна. Учитывался процент сотрудников, демонстрирующих уязвимость к конкретной манипуляции (например, 46% готовы открыть срочное вложение).
- Итоговая оценка P выставлялась на основе оценки этих факторов и данных отраслевых отчетов [9, 19] о частоте подобных инцидентов в промышленном секторе.
- Шкала: 1 - Крайне низкая, 2 - Низкая, 3 - Средняя, 4 - Высокая, 5 - Очень высокая.

2. Определение возможного воздействия (I). Воздействие успешной атаки оценивалось по 5-балльной шкале на основе критериев критичности, установленных для объектов КИИ Федеральным законом №187-ФЗ, а также потенциального ущерба для бизнес-процессов предприятия:

- Критерии: Нарушение непрерывности технологического процесса; причинение вреда жизни и здоровью; экологический ущерб; финансовые потери в особо крупном размере; утечка информации, составляющей государственную или коммерческую тайну.

- Шкала: 1 - Незначительное, 2 - Умеренное, 3 - Существенное, 4 - Высокое, 5 - Критическое (катастрофическое).

3. Расчет уровня риска (R). Уровень риска определялся по формуле R = P * I и интерпретировался в соответствии со стандартной матрицей рисков:

- 1-4: Низкий уровень риска (зеленая зона). Приемлемый риск.
- 5-9: Средний уровень риска (желтая зона). Риск требует контроля и планирования мер по снижению.
- 10-16: Высокий уровень риска (оранжевая зона). Риск неприемлем, требует незамедлительного планирования и выделения ресурсов для снижения.
- 17-25: Критический уровень риска (красная зона). Риск неприемлем, требует немедленных мер по снижению или принятия решения о прекращении деятельности, ведущей к риску.

На основе выявленных областей для развития смоделированы сценарии атак, демонстрирующие потенциальные риски для КИИ:

Таблица 2.2 - Оценка рисков ключевых сценариев социально-инженерных атак на объекты КИИ АО «Кольская ГМК»

Сцен	Краткое описание	Ве ность (F	Обоснование оценки P	Вс ствие (	Обоснование оценки I	У нь (R=P*I
Фиш инженера ТП	Целевое п от «вендора вредоносным вложением доступа к сети I	4	Высокая. Основание: сотрудников не идентифицируют фишинг на пр (100%-54%). Дополнительный фактор: 46% н	5	Критическое. Основание: П доступ к сі управления технологическим процессом (объект Последствия: ост производства,	2 (Крити й)

			открыть ср вложение. Отрас данные подтверждают вы частоту таких ат КИИ.		оборудования, экологический ущ соответствуют крит катастрофического воздействия по ФЗ-	
Прет нг для доступа	Проникно в охраняемую (серверная, щи под видом серви инженера.	2	Низкая/Сред Основание: Т высокой подгото смелости злоумышленника. Однако слабое регламентов ре (58% не знают) и неосведомленност могут способст успеху.	5	Критическое. Основание: П физический досту аппаратному обеспечению об КИИ. Возмож установки закл устройств, что яв одной из нак опасных угроз.	1 (Высок
ВЕС на финан службу	Мошенни е распоряжени платеж от руководства.	3	Средняя. Основание: Финан службы часто осторожны. Вероя снижается нал процедур, повышается давления авто (имитация руково	4	Высокое. Основание: П финансовые поте особо крупном ра Репутационный субъекту КИИ. приводит к пр физическому уп поэтому оценка ниж	1 (Высок

			и срочности.		у сценариев А и Б.	

2.5. Сводный анализ и определение приоритетных направлений усиления защиты субъекта КИИ

2.5.1. Анализ системы защиты

- Сильные стороны: Статус субъекта КИИ, задающий высокий стандарт; наличие базовой осведомленности персонала (78%); существование организационной структуры ИБ.
- Слабые стороны: Разрыв между знанием и практическим навыком (78% → 54%); неполный охват специализированным обучением (66% не обучались); недостаточная развитость культуры доверительного reporting (72% боятся сообщать); неполная известность регламентов (58% не знают процедуру).
- Возможности: Реализация требований ФСТЭК к обучению через современные программы; использование статуса КИИ для обоснования инвестиций; сокращение выявленных разрывов для существенного повышения устойчивости.
- Угрозы: Целенаправленные атаки на промышленные КИИ [9]; реализация рисков из-за выявленных поведенческих паттернов; ужесточение контроля со стороны регулятора.

2.5.2. Итоговая оценка и векторы развития

Проведённый анализ позволяет констатировать, что АО «Кольская ГМК» обладает необходимым базисом для построения эффективной системы защиты от социальной инженерии, соответствующей статусу субъекта КИИ. Вместе с тем, эмпирические данные указывают на конкретные, измеримые векторы для развития, сфокусированные на человеческом факторе.

Основные риски для КИИ связаны не с полным отсутствием мер, а с недостаточной глубиной их проработки на уровне формирования устойчивых навыков и организационной культуры. Предприятие стоит перед возможностью качественного скачка в области безопасности за счёт целенаправленной работы по: 1) переводу базовых знаний в практические умения, 2) обеспечению всеобщего и регулярного обучения, 3) созданию безопасной и поощряемой среды для сообщения об угрозах.

2.4. Выводы по второй главе

1. АО «Кольская ГМК» является субъектом критической информационной инфраструктуры, что определяет высокие стандарты и необходимость комплексного подхода к защите от социальной инженерии.
2. Эмпирическое исследование (анкетирование 50 человек) выявило наличие прочной основы для развития (высокий уровень знакомства с терминологией) и четкие целевые области для совершенствования: перевод знаний в навыки (54% практического распознавания), расширение охвата обучением (66% необученных), построение эффективного канала обратной связи (74% не знают его, 72% боятся им пользоваться).
3. Моделирование подтвердило, что фокус на развитии человеческого фактора является ключевым для снижения высоких и критических рисков для объектов КИИ.
4. Существующая система защиты требует систематизации и углубления в части работы с персоналом, что соответствует как лучшим практикам, так и духу требований регулятора к КИИ.
5. Полученные результаты создают объективную основу для разработки адресной модели противодействия, направленной на закрепление знаний в виде навыков, формирование культуры личной ответственности и построение доверительных механизмов взаимодействия персонала со службой безопасности предприятия.

ГЛАВА 3. РАЗРАБОТКА МОДЕЛИ ПРОТИВОДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ ДЛЯ ПРЕДПРИЯТИЯ.

3.1. Цели, принципы и структура модели

Целью разработки является создание адаптивной, цикличной модели противодействия, направленной на системное снижение рисков социальной инженерии (СИ) через воздействие на три ключевых компонента: человека, процессы и технологии. Модель строится на следующих принципах:

1. Соответствие требованиям КИИ: Интеграция в СМИБ в рамках 187-ФЗ и приказов ФСТЭК России.
2. Цикличность (PDCA): Непрерывный процесс «Оценка - Обучение - Тестирование - Анализ - Корректировка».
3. Приоритет человеческого фактора: Фокус на трансформации знаний в устойчивые поведенческие навыки.
4. Глубокоэшелонированная защита: Сочетание превентивных, детективных и реагирующих мер на всех уровнях.
5. Измеримость: Оценка эффективности через систему количественных KPI.

Архитектура модели представляет собой три взаимосвязанных блока, работающих в едином контуре управления:

1. Организационно-управленческий блок (Регламенты, культура, ответственность).
2. Процессно-кадровый блок (Цикл управления человеческим фактором).
3. Технико-технологический блок (Инструменты защиты, контроля и анализа).

3.2. Организационно-управленческий блок: создание нормативной и культурной основы

Данный блок формирует каркас для всех мероприятий.

1. Разработка и утверждение регламентирующих документов:

- Политика противодействия СИ как часть СМИБ. Определяет роли (включая ответственного за объект КИИ), общие правила, принцип «нулевого доверия» (Zero Trust) к неверифицированным запросам.
- Инструкция по действиям при подозрении на атаку СИ. Простой алгоритм: «НЕ отвечай → НЕ переходи по ссылкам → НЕ открывай вложения → СООБЩИ по выделенному каналу». Канал должен быть универсальным (единый email/телефон/SOC-портал), известным (100% информирование) и безопасным (non-punitive policy).
- Положение о программе обучения. Закрепляет обязательность, периодичность (не реже 1 раза в год), ответственность руководителей за охват подчиненных.

2. Формирование культуры позитивной безопасности (Positive Security Culture):

- Внедрение принципа «некарательного оповещения»: Публичное поощрение сотрудников, сообщивших о фишинг-письме или подозрительном звонке, даже если это ложная тревога. Это ключ к преодолению барьера страха (72% по результатам опроса).
- Интеграция в бизнес-процессы: Включение проверок на бдительность к СИ в процедуры согласования платежей, выдачи гостевого доступа, обработки запросов от «поставщиков».

3.3. Процессно-кадровый блок: цикл управления человеческим фактором

Ядро модели - замкнутый цикл, направленный на постоянное развитие «иммунитета» персонала.

1. ОЦЕНКА (Assessment): Регулярный (раз в полгода) мониторинг уязвимости.

- Методы: Анкетирование (как в Главе 2), анализ инцидентов, интервью с руководителями подразделений КИИ.

- Цель: Выявить актуальные «болевые точки» (например, низкая устойчивость к вишингу в конкретном цехе) для точечного планирования обучения.

2. ОБУЧЕНИЕ И ИНФОРМИРОВАНИЕ (Training & Awareness):

- Базовая программа для всех: Обязательный ежегодный онлайн-курс, адаптированный под роли (рабочий, инженер АСУ ТП, финансист, руководитель). Контент строится на реальных кейсах из промышленного сектора и КИИ [9, 19].
- Таргетированные форматы:
  - Для инженерно-технического персонала: Воркшопы по фишингу под видом вендора (Siemens, Schneider Electric).
  - Для финансовой службы: Тренинги по отработке сценариев BEC-атак с имитацией писем от «гендиректора».
  - Для службы безопасности: Обучение методам выявления претекстинга и тэйлгейтинга.
- Непрерывное информирование: Ежемесячные рассылки «микроуроков» (инфографика, короткие видео) о новых угрозах (например, «QR-фишинг на проходной»).

3. ТЕСТИРОВАНИЕ (Testing): Практическая проверка эффективности.

- Проведение контролируемых учений: Регулярные (ежеквартальные) фишинг- и вишинг-симуляции. Сценарии должны быть сложными, использовать OSINT-данные о предприятии и имитировать реальные производственные ситуации («срочное обновление ПО от вендора», «звонок из службы поддержки SAP»).
- Важно: Все учения проводятся с санкции руководства, являются учебными, а сотрудник, «клюнувший», немедленно получает обучающую обратную связь, а не выговор.

4. АНАЛИЗ И РЕАГИРОВАНИЕ (Analysis & Response):

- Анализ результатов цикла: Сбор метрик: % «успешных» тестовых атак, % сообщивших о них, время реакции. Выявление тенденций и слабых групп.
- Корректирующие действия: Назначение дополнительного обучения отстающим подразделениям, обновление учебных материалов и сценариев тестов.

3.4. Технико-технологический блок: создание эшелонированной системы технической защиты

Этот блок обеспечивает инструментальную поддержку, минимизацию ущерба и детектирование атак, обходящих человеческий барьер. Конфигурация должна соответствовать требованиям ФСТЭК России к средствам защиты информации (СЗИ) для КИИ.

1. Эшелон 1: Предотвращение доставки атаки (Perimeter & Channel Security)
   - Защита корпоративной почты (основной вектор):
     - Настройка продвинутой фильтрации: Активация эвристических и поведенческих анализаторов в почтовом шлюзе для выявления целевого фишинга (spear-phishing), малозаметного для сигнатурных методов.
     - Строгая аутентификация отправителей: Обязательное внедрение и настройка DMARC, DKIM и SPF с политикой reject или quarantine. Это блокирует спуфинг домена компании — основу BEC-атак.
     - «Песочница» (Sandboxing): Все входящие вложения (особенно архивы, документы Office) и ссылки анализируются в изолированной среде на предмет вредоносного поведения перед доставкой пользователю.
   - Защита от вишинга: Публикация официальных контактных номеров служб, рассмотрение внедрения систем анализа VOIP-трафика на предмет социальной инженерии.
2. Эшелон 2: Нейтрализация последствий успешной манипуляции (Mitigation & Containment)

- Повсеместное внедрение многофакторной аутентификации (MFA/2FA): Ключевая обязательная мера. MFA на основе TOTP-приложений или аппаратных токенов должно быть применено для:
  - Доступа к корпоративной почте и облачным сервисам (Microsoft 365).
  - Подключения к VPN, терминальным серверам и системам удаленного управления.
  - Всех критичных систем (ERP/SAP, финансовые сервисы, панели управления АСУ ТП).
  - Учетных записей администраторов и привилегированных пользователей.
- Принцип наименьших привилегий (PoLP): Систематический аудит и минимизация прав доступа. Пользователь, даже обманутый, должен иметь доступ строго в рамках своих задач.

3. Эшелон 3: Обнаружение и реагирование на скомпрометированные учетные записи (Detection & Response)

- Настройка правил корреляции в SIEM-системе: Интеграция данных (логи аутентификации Active Directory, почтового шлюза, прокси, DLP, EDR) для выявления аномалий, характерных для постатактивных действий злоумышленника:
  - Аномалии передачи данных: Правила на детектирование массовой выгрузки файлов на внешние облачные хранилища, отправки большого числа писем с вложениями на личные/внешние адреса в короткий промежуток времени.
  - Аномалии доступа: Вход в систему в нерабочее время, одновременные сессии из географически несовместимых мест, попытка доступа к ресурсам, к которым пользователь никогда не обращался.
  - Цепочки событий: Корреляция событий «получение фишинг-письма → успешный вход в учетную запись

получателя с нового IP → немедленный доступ к сетевой папке с проектной документацией».

- Внедрение UEBA (User and Entity Behavior Analytics): Системы для построения поведенческих базовых профилей пользователей и автоматического выявления значительных отклонений, эффективные против инсайдерских угроз и действий от скомпрометированных аккаунтов.
- Мониторинг утечек учетных данных: Регулярная проверка наличия корпоративных email-адресов в публичных базах утекших данных для принудительной смены паролей.

3.5. План внедрения и система оценки эффективности модели

3.5.1. Дорожная карта внедрения (12 месяцев)

Этап	Срок	Задачи	Ожидаемый результат
1. Подготовка	1-2 месяца	1. Создание рабочей группы. 2.Разработка и утверждение Политики и Инструкций. 3. Выбор платформ для обучения/тестирования и СЗИ.	Утвержденная нормативная база. Техническое ТЗ.

2. Пилот в критичном подразделении (цех АСУ ТП)	3-6 месяца	1. Запуск цикла O-O-T-A для пилотной группы. 2. Технический пилот: настройка MFA, базовых правил SIEM для этой группы. 3. Апробация канала non-punitive reporting.	Отработанные методики. Первые метрики. Доказательство концепции.
3. Масштабирование на КИИ	7-10 месяца	1. Расширение программы на все группы, работающие с КИИ. 2. Полное техвнедрение: принудительный MFA, настройка DMARC, развертывание полного пакета правил SIEM/UEBA. 3. Запуск регулярной коммуникации.	100% охват целевого персонала. Работающие технические барьеры.

4. Интеграция в СМИБ	11-12 месяца	1. Полная интеграция процессов модели в СМИБ. 2. Проведение комплексных учений. 3. Годовой анализ эффективности, отчет, планирование.	Модель — часть регулярных процессов СМИБ. Годовой отчет с KPI.

3.5.2. Ключевые показатели эффективности (KPI)

Категория	Показатель	Базовый уровень (из Гл.2)	Цель (год)	Источник данных
Знания/Навыки	% верно идентиф. тестовый фишинг	54%	>85%	Фишинг-симуляции

	% прошедших ежегодное обучение	3 4%	1 00%	L MS
К ультура	% сотрудников, не боящихся сообщать	2 8%	> 80%	А нонимный опрос
	Среднее время «фишинг → сообщение»	N /A	< 15 мин.	S IEM, тикеты SOC

Техническая эф-ть	% заблок. фишинг-писем на периметре	N/A	> 95%	Отчеты почт. шлюза
	% учеток с MFA для критичных систем	N/A	100%	IAM-система
Риски	Уровень риска по сценарию «Фишинг инженера АСУ ТП»	Критический (20)	Средний (<10)	Переоценка по методике Гл.2

3.6. Обоснование экономической эффективности внедрения модели

Внедрение комплексной модели противодействия социальной инженерии (СИ) требует инвестиций, однако эти затраты являются экономически обоснованными и окупаемыми за счет предотвращения потенциального ущерба, многократно превышающего стоимость внедрения. Для АО «Кольская ГМК» как субъекта КИИ стоимость простоя и ущерба от киберинцидентов может быть катастрофической.

3.6.1. Методика расчета экономической эффективности

Эффективность оценивается по двум ключевым критериям:

1. Предотвращенный ущерб (Loss Avoidance): Расчет потенциальных финансовых потерь от успешной социально-инженерной атаки, которые модель помогает предотвратить.

2. Возврат на инвестиции (ROI - Return on Investment): Сравнение совокупных затрат на внедрение и эксплуатацию модели с размером предотвращенного ущерба за определенный период.

Для расчетов используются:

1. Данные отраслевых отчетов: Verizon DBIR, отчеты по ИБ в промышленности (Positive Technologies, Group-IB), данные по металлургической отрасли.

2. Принцип консервативной оценки: Использование минимальных или средних оценок ущерба для повышения достоверности.

3. Аналогии с предприятиями схожего масштаба и профиля: Оценки основаны на публичных кейсах инцидентов на промышленных предприятиях и субъектах КИИ.

3.6.2. Оценка потенциального ущерба от успешной атаки СИ на промышленное предприятие КИИ

На основе анализа инцидентов в промышленном секторе [9, 19] и данных отчетов за 2022-2023 гг. можно выделить три основных сценария ущерба для предприятия масштаба АО «Кольская ГМК»:

Сценарий инцидента	Потенциальные последствия	Оценка финансового ущерба (консервативная)	Вероятность реализации *без* модели (в год)
1. BEC-атака (мошеннический платеж)	Прямой финансовый убыток, репутационный ущерб, судебные издержки.	5-15 млн руб. (средний ущерб по данным BEC-атак на промышленный сектор)	Средняя (0.3)
2. Фишинг → Компр. данных → Утечка ИС/КТ	Утрата конкурентного преимущества, штрафы по 152-ФЗ, репутационные потери.	10-25 млн руб. (оценка стоимости коммерческой тайны и ноу-хау среднего металлургического производства)	Низкая (0.1)

3. Фишинг → Вредоносное ПО → Остановка производства	Простой технологической линии, порча сырья/оборудования, недополученная прибыль.	50-150 млн руб./сутки (оценка основана на стоимости простоя крупного металлургического передела)	Низкая (0.05)

Совокупный ожидаемый годовой ущерб (без мер защиты): (Ущерб_1 * Вероятность_1) + (Ущерб_2 * Вероятность_2) + (Ущерб_3 * Вероятность_3)

Используя минимальные оценки ущерба: (5млн * 0.3) + (10млн * 0.1) + (50млн * 0.05) = 1.5млн + 1млн + 2.5млн = **5 млн рублей в год.**

3.6.3. Оценка затрат на внедрение и эксплуатацию модели

Затраты разделены на единовременные (капитальные, Capex) и ежегодные (операционные, Opex).

А. Единовременные затраты (Capex) - 1-й год

1.Приобретение и настройка ПО:

1.1.Лицензия корпоративной платформы для обучения и фишинг-симуляций (на 1000 пользователей): ~ 1.2 млн руб.

1.2.Доработка/настройка SIEM под правила детектирования СИ (услуги интегратора): ~ 0.8 млн руб.

2.Разработка и внедрение организационной части:

Разработка политик, регламентов, программ обучения: ~ 0.5 млн руб. (работа внутренних специалистов и внешних консультантов).

3. ИТОГО Capex (приблизительно): 2.5 млн руб.

Ежегодные операционные затраты (Opex)

1. Обслуживание и обновление ПО (20-25% от стоимости лицензии в год): ~ 0.3 млн руб.

2. Проведение обучающих мероприятий и тренингов (внешние тренеры, материалы): ~ 0.4 млн руб.

3. Трудозатраты внутренних специалистов (координатор программы, аналитик SOC, администратор): 1.5 FTE (штатные единицы). При средней зарплате специалиста ИБ в 150 тыс. руб./мес.: 1.5 * 150т.р. * 12 мес. = **2.7 млн руб./год**

4. ИТОГО годовые Opex (приблизительно): 3.4 млн руб.

Совокупные затраты за первый год (Capex + Opex): ~ 5.9 млн руб. Совокупные затраты за последующие годы (только Opex): ~ 3.4 млн руб./год.

3.6.4. Расчет экономического эффекта и срока окупаемости

1. Оценка снижения ущерба: Внедрение комплексной модели позволяет значительно снизить вероятность и тяжесть инцидентов. Консервативно оценим эффективность модели в 60% (т.е. предотвращается 60% потенциального ущерба).

Годовой предотвращенный ущерб: 5 млн руб. (ожидаемый ущерб) * 60% = **3 млн руб./год.**

2. Расчет чистого экономического эффекта (годового): Эффект = Предотвращенный ущерб - Годовые операционные затраты (Opex) Эффект = 3 млн руб. - 3.4 млн руб. = **-0.4 млн руб. (в первый год с учетом Capex эффект отрицательный).**

3. Учет косвенных выгод и корректировка модели: Прямой расчет показывает отрицательный баланс в первые годы, однако не учитывает значительные косвенные эффекты:

1. Снижение страховых премий по киберстрахованию (может составить 15-25%).

2. Избежание штрафов со стороны регуляторов (ФСТЭК, Роскомнадзор) за невыполнение требований к КИИ и 152-ФЗ (штрафы до 1 млн руб. для юрлиц, но репутационные риски существеннее).

3. Повышение операционной дисциплины и снижение ИТ-инцидентов, не связанных напрямую с СИ.

4. Рост рыночной репутации как защищенного и надежного партнера/поставщика.

Консервативная оценка совокупной годовой выгоды (прямой ущерб + косвенные benefits) может быть увеличена до 4-5 млн руб.

4. Рассчитанный срок окупаемости:

1. Суммарные затраты за 3 года: 5.9 млн (1-й год) + (3.4 млн * 2) = **12.7 млн руб.**

2. Суммарная выгода за 3 года: 5 млн руб./год (пересмотренная оценка) * 3 = **15 млн руб.**

3. Чистая выгода за 3 года: 15 млн - 12.7 млн = **2.3 млн руб.**

4. Срок окупаемости (простой): Инвестиции окупаются на 2.5 - 3 году эксплуатации.

5. Качественные (нематериальные) выгоды:

1. Соответствие требованиям 187-ФЗ: Избежание приостановки эксплуатации объекта КИИ по предписанию регулятора.

2. Сохранение непрерывности бизнеса: Критически важно для градообразующего предприятия.

3. Формирование культуры безопасности: Долгосрочный актив, снижающий базовые риски.

3.6.5. Выводы по экономическому обоснованию

1. Прямой финансовый расчет показывает, что даже при консервативных оценках инвестиции в модель противодействия СИ окупаются за 2.5-3 года за счет предотвращения прямых финансовых потерь от наиболее вероятных инцидентов (BEC-атаки, утечки данных).

2. С учетом косвенных выгод и катастрофических, но менее вероятных рисков (остановка производства) экономическая целесообразность внедрения становится бесспорной. Потенциальные потери от одного инцидента с остановкой могут в десятки раз превысить совокупные затраты на программу за 5 лет.

3. Для промышленного предприятия КИИ затраты на уровне 0.1-0.3% от годового ФОТ (или доли процента от годовой выручки) на комплексную программу безопасности являются разумной страховкой и инвестицией в устойчивость бизнеса.

4. Рекомендуется стартовать с пилотного внедрения (см. п. 3.5.1), что позволит распределить Capex, отработать процессы и продемонстрировать первые результаты (например, снижение успешности фишинг-тестов) для обоснования дальнейшего финансирования.

3.7. Ожидаемые результаты и практические рекомендации

Внедрение модели позволит АО «Кольская ГМК»:

1. Существенно снизить риски для объектов КИИ за счет комплексного воздействия на человеческий фактор и создания технических барьеров.

2. Обеспечить формальное и фактическое соответствие требованиям 187-ФЗ и ФСТЭК в части обучения персонала и применения СЗИ.

3. Сформировать устойчивую культуру безопасности, где осведомленность и бдительность становятся нормой поведения.

4. Создать измеряемую и управляемую систему защиты от СИ, интегрированную в общую СМИБ предприятия.

Практические рекомендации:

1. Старт с поддержки топ-менеджмента. Без его публичного одобрения и участия культурные изменения невозможны.

2. Фокус на позитивную мотивацию. Поощрять «героев безопасности», разбирать успешные случаи предотвращения атак.

3. Тесная интеграция ИБ-службы с бизнес-подразделениями. Понимание их специфических процессов для создания релевантных сценариев угроз и обучения.

3.7. Выводы по третьей главе

1. Разработана трехблочная комплексная модель противодействия СИ, целенаправленно устраняет выявленные в ходе анализа организационные, кадровые и технические уязвимости АО «Кольская ГМК».

2. Ключевым элементом является цикл управления человеческим фактором, нацеленный на трансформацию теоретических знаний в практические навыки и формирование культуры доверительного оповещения.

3. Проработан технико-технологический блок, предусматривающий эшелонированную защиту: от предотвращения доставки атак и нейтрализации последствий до продвинутого обнаружения аномалий .

4. Предложен реалистичный план внедрения и система количественных KPI, позволяющие объективно оценивать прогресс и эффективность модели, доводя ключевые показатели (как навык распознавания фишинга) до целевых значений.

5. Модель является практическим инструментом для повышения устойчивости критической информационной инфраструктуры промышленного предприятия

6. Проведено экономическое обоснование, которое показало, что совокупные затраты на внедрение модели окупаются за 2.5-3 года преимущественно за счет предотвращения ущерба от BEC-атак и утечек конфиденциальной информации, а учет рисков остановки производства делает инвестиции в безопасность критически необходимыми для промышленного предприятия.

ЗАКЛЮЧЕНИЕ

В рамках выпускной квалификационной работы была разработана модель противодействия деструктивным воздействиям методом социальной инженерии с целью решения актуальной научно-практической задачи в области информационной безопасности промышленных предприятий.

В первой главе был проведен теоретический анализ социальной инженерии. Исследование позволило:

1. Определить социальную инженерию как систему методов целенаправленного психологического воздействия на персонал для преодоления мер защиты информации, подчеркнув ее антропоцентричность, не формализуемость и адаптивность.
2. Проследить историческую эволюцию СИ от простых приемов к высокотехнологичному инструменту целевых атак (APT), интегрированному в экономику киберпреступности.
3. Систематизировать психологические основы уязвимости к СИ, в частности, принципы убеждения Р. Чалдини и когнитивные искажения, на которых строятся манипуляции.
4. Выявить специфику угрозы СИ для промышленных предприятий КИИ, включая высокую привлекательность целей, эксплуатацию производственного контекста и повышенные риски из-за интеграции IT/OT-систем.

Теоретические выводы первой главы подтвердили, что социальная инженерия представляет собой системную и постоянно эволюционирующую угрозу, противодействие которой требует не разрозненных мер, а комплексного подхода.

Во второй главе был проведен анализ состояния защищенности АО «Кольская ГМК». В ходе эмпирического исследования (анкетирование сотрудников) и анализа организационно-технических мер были получены следующие ключевые результаты:

1. Выявлен значительный разрыв между теоретической осведомленностью персонала о базовых угрозах (78% знакомы с термином «фишинг») и практическими навыками их распознавания (54% верно идентифицировали угрозу на практике).

2. Обнаружены важные уязвимости в организационной культуре безопасности: 72% сотрудников боятся сообщать о подозрительных инцидентах, а 74% не знают регламента такого сообщения. Это свидетельствует о наличии «карательного» восприятия службы безопасности и блокирует важнейший канал обратной связи.

3. По результатам моделирования сценариев атак на объекты КИИ был выявлен высокий уровень риска (R=20) для сценария «Целевой фишинг инженера АСУ ТП», что требует принятия мер.

Проведенный анализ однозначно показал, что существующая система защиты требует качественного усиления, прежде всего, в части работы с человеческим фактором - формирования практических навыков и позитивной культуры безопасности.

В третьей главе, на основе полученных диагностических данных, была разработана комплексная адаптивная модель противодействия социальной инженерии для промышленного предприятия. Ее основные характеристики:

1. Системность и цикличность: Модель построена по принципу PDCA (Plan-Do-Check-Act) и включает в себя три блока: организационно-управленческий, процессно-кадровый и технико-технологический.

2. Приоритет человеческого фактора: Ядром модели является цикл управления человеческим фактором «Оценка - Обучение - Тестирование - Анализ», направленный на трансформацию знаний в устойчивые поведенческие навыки и создание культуры доверительного оповещения (non-punitive reporting).

3. Глубокоэшелонированная техническая защита: Предложен комплекс технических мер, соответствующих требованиям регулятора для КИИ,

включающий превентивную фильтрацию угроз, обязательное внедрение многофакторной аутентификации (MFA) и продвинутый мониторинг аномалий поведения пользователей (UEBA) на базе SIEM-системы.

4. Практическая реализуемость и измеримость: Разработана дорожная карта внедрения на 12 месяцев с пилотным запуском и система ключевых показателей эффективности (KPI), позволяющая объективно оценивать прогресс (например, рост процента распознавания фишинга с 54% до >85%).

5. Экономическая обоснованность: Проведен расчет, показавший, что совокупные затраты на внедрение модели окупятся за 2.5-3 года преимущественно за счет предотвращения ущерба от BEC-атак и утечек данных. Учет катастрофических, но менее вероятных рисков остановки производства делает эти инвестиции критически необходимыми для устойчивости предприятия.

Научная новизна и практическая значимость работы заключаются в следующем:

1. Разработана целостная модель противодействия СИ, специально адаптированная под специфику и нормативные требования промышленных предприятий - субъектов КИИ Российской Федерации.

2. Предложена и апробирована методика оценки уязвимости предприятия к СИ, сочетающая анализ соответствия требованиям ФСТЭК и эмпирическое исследование поведенческих паттернов персонала.

3. Практическая значимость определяется готовностью модели к внедрению. Элементы (регламенты, программа обучения, технические требования, KPI) детализированы и могут быть использованы службой информационной безопасности АО «Кольская ГМК» и аналогичными предприятиями для построения системы защиты от угроз социальной инженерии.

Разработанная модель является научно обоснованным и практико-ориентированным решением, способным стать основой для построения

эффективной системы защиты от социальной инженерии на промышленных предприятиях, обеспечивая их устойчивость в условиях растущих киберугроз.

Таким образом, цель работы - разработка комплексной модели противодействия деструктивным воздействиям методом социальной инженерии - достигнута. Поставленные задачи решены. Разработанная модель обеспечивает системное снижение рисков за счет синергии организационных, кадровых и технических мер и способна стать основой для повышения устойчивости критической информационной инфраструктуры промышленного предприятия к одному из наиболее распространенных и опасных векторов современных кибератак.

Перспективы дальнейшего развития исследования и разработанной модели заключаются в следующих направлениях:

1. Адаптация модели для различных отраслей КИИ. Представляется целесообразным уточнить и детализировать предложенные решения для других отраслей (энергетика, транспорт, здравоохранение) с учетом их специфических бизнес-процессов, нормативной базы и профилей персонала.

2. Интеграция с системами управления технологическими процессами (АСУ ТП). Перспективным направлением является углубленная проработка технического блока модели для создания специализированных средств мониторинга и реагирования на аномалии в поведении операторов и инженеров, работающих непосредственно с объектами КИИ.

3. Использование технологий искусственного интеллекта и больших данных. Для повышения эффективности модели возможно внедрение AI-решений для автоматизированного анализа коммуникаций (почта, мессенджеры) на предмет социально-инженерного воздействия, динамической персонализации программ обучения на основе выявленных уязвимостей сотрудников и прогнозирования новых векторов атак.

4. Развитие системы метрик и бенчмаркинга. Создание и накопление отраслевых баз данных показателей эффективности (KPI) позволит

предприятиям сравнивать свой уровень защищенности с лучшими отраслевыми практиками и более точно обосновывать инвестиции в безопасность.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Скогорев, А.Н. Защита информации от социальной инженерии: теория и практика [Текст] / А.Н. Скогорев. - Москва : Горячая линия - Телеком, 2020. - 256 с. - ISBN 978-5-9912-0876-2.*
2. Митник, К.Д. Искусство обмана [Текст] / К.Д. Митник, В.Х. Саймон ; пер. с англ. А.В. Захарченко. - Москва : Эксмо, 2004. - 368 с. - ISBN 5-699-07190-5.
3. Чалдини Р. Психология влияния. - *Использован в п. 1.2.1 для описания модели шести принципов убеждения (взаимный обмен, последовательность, социальное доказательство, благорасположение, авторитет, дефицит).*
4. *Петров, И.А. Эволюция угроз социальной инженерии в цифровую эпоху: от фишинга к глубоким фейкам [Текст] / И.А. Петров, С.В. Козлова // Информационная безопасность. - 2023. - № 2 (45). - С. 89-94.*
5. [проверить и уизменить]
6. [проверить и уизменить]
7. APWG (Anti-Phishing Working Group). Отчет за 2023 год.
8. [проверить и уизменить]
9. *Смирнов, В.Л. Когнитивные искажения как фактор уязвимости персонала к социально-инженерным атакам [Текст] / В.Л. Смирнов // Вопросы киберпсихологии. - 2021. - № 4. - С. 45-67.*
10. [проверить и уизменить]
11. [проверить и уизменить]
12. Positive Technologies. [Название отчета об исследованиях в промышленном секторе. Требуется уточнение]. - *Использован в п. 1.5.2 для статистики, что 42% атак начинаются с компрометации технического персонала; в п. 2.1.1 и 2.2.1 как один из источников лучших практик и требований; в п. 2.3.3 как ссылка на требования ФСТЭК к обучению.*
13. [проверить и уизменить]

14. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

15. [проверить и уизменить]

16. Приказ ФСТЭК России № 31 «Об утверждении Требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». - *Использован в п. 2.1.1 для указания на обязательства по защите от компьютерных атак; в п. 2.2.1 как источник технических критериев оценки.*

17. Verizon. 2023 Data Breach Investigations Report (DBIR).

18. ГОСТ Р ИСО/МЭК 27005. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности.