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 методики защиты информации от целевого фишинга в автоматизированной системе управления предприятием**»**

Исполнитель _____ Купалов Никита Дмитриевич

(подпись) (фамилия, имя, отчество)

Руководитель _____ Переспелов Анатолий Витальевич

(подпись) (фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____ Лепешкин Олег Михайлович

(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: Купалову Никите Дмитриевичу

(фамилия, имя, отчество)

1. Тема Разработка методики защиты информации от целевого фишинга в автоматизированной системе управления предприятием

закреплена приказом ректора Университета от «___» _____20___ года, № _____

2. Срок сдачи законченной работы «___» _____20___ года

3. Исходные данные к выпускной квалификационной работе:

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

Введение. Цели и задачи ВКР

Глава 1 Целевой фишинг как доминирующая угроза безопасности современного предприятия и анализ существующих подходов к защите

(наименование главы)

Глава 2 Разработка методики защиты от целевого фишинга для АСУП

(наименование главы)

Глава 3 Практическая реализация и апробация методики защиты от целевого фишинга в АСУП

(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

_____ _____

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

Задание принял к исполнению «___» 20___ года

Студент Купалов Никита Дмитриевич, ИБ-С20-1 _____

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

РЕФЕРАТ

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

РАЗРАБОТКА МЕТОДИКИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ.

Объект исследования - процессы обеспечения информационной безопасности в автоматизированных системах управления предприятием (АСУП).

Предмет исследования – методы и средства защиты информации от целевых фишинговых атак, нацеленных на персонал, работающий с АСУП.

Цель исследования разработка научно-обоснованной и практико-ориентированной методики защиты информации от целевого фишинга в АСУП.

Задачи исследования:

1. Провести анализ угрозы целевого фишинга и существующих подходов к защите.
2. Разработать комплексную методику защиты, включающую ролевую модель оценки рисков, программу обучения персонала, технический контур и регламенты реагирования.
3. Провести апробацию методики на модели условного предприятия и оценить её эффективность.

Разработана методика защиты информации от целевого фишинга в автоматизированной системе управления предприятием

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Автоматизированные системы управления предприятием (АСУП) стали технологическим стержнем современного бизнеса, обеспечивая оперативность, прозрачность и эффективность ключевых процессов — от логистики и производства до финансового планирования и управления персоналом. Концентрация критически важных данных (коммерческая тайна, персональные данные, финансовые отчёты) в рамках единой цифровой среды АСУП радикально повышает операционную эффективность, но одновременно превращает её в высокоценную цель для киберпреступников. В условиях стремительной цифровой трансформации и геополитической нестабильности, особенно актуальной для российской экономики, угрозы информационной безопасности приобретают масштаб прямого риска для непрерывности бизнеса и национальной экономической стабильности.

Среди всего спектра киберугроз целевой фишинг (spear phishing) выделяется как доминирующий и наиболее опасный вектор целевой атаки на организации. Эволюционировав от примитивного мошенничества до высокотехнологичного инструмента, сочетающего искусственный интеллект, глубокую аналитику открытых данных (OSINT) и изощрённую социальную инженерию, современный фишинг целенаправленно атакует не технические уязвимости ПО, а ключевое звено любой системы защиты — человеческий фактор. Сотрудник, работающий с АСУП, под давлением искусственно созданной срочности или ложного авторитета может стать невольным посредником в обходе всех периметровых защит, что ведёт к катастрофическим последствиям: хищению денежных средств (BEC-атаки), утечке конфиденциальной информации, внедрению вредоносного ПО и полной компрометации корпоративной сети.

Объект исследования - процессы обеспечения информационной безопасности в автоматизированных системах управления предприятием (АСУП).

Предмет исследования – методы и средства защиты информации от целевых фишинговых атак, нацеленных на персонал, работающий с АСУП.

Цель исследования разработка научно-обоснованной и практико-ориентированной методики защиты информации от целевого фишинга в АСУП.

Задачи исследования:

1) Провести анализ угрозы целевого фишинга и существующих подходов к защите.

2) Разработать комплексную методику защиты, включающую ролевую модель оценки рисков, программу обучения персонала, технический контур и регламенты реагирования.

3) Провести апробацию методики на модели условного предприятия и оценить её эффективность.

Методы исследования: методы теоретического анализа, методы системного анализа, метод моделирования и экономического обоснования.

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

В первой главе проведен комплексный анализ угрозы целевого фишинга для АСУП, исследованы её эволюция, психологические и технические механизмы, а также выполнен критический обзор существующих стандартов информационной безопасности.

Вторая глава включает разработку комплексной методики защиты от целевого фишинга, содержащей ролевую модель оценки рисков, архитектуру адаптивной программы обучения персонала, проект технического контура защиты и регламенты оперативного реагирования на инциденты.

Третья глава посвящена практической апробации предложенной методики на модели условного предприятия, оценке её количественной и экономической эффективности, а также формулированию рекомендаций по внедрению.

В заключении представлены итоги исследования, подтверждающие эффективность разработанной методики, и основные выводы по проделанной работе.

ГЛАВА 1. ЦЕЛЕВОЙ ФИШИНГ КАК ДОМИНИРУЮЩАЯ УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОГО ПРЕДПРИЯТИЯ И АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К ЗАЩИТЕ

1.1. Возникновение и эволюция фишинга: от массовых рассылок к гибридным AI-атакам

Фишинг прошёл путь от примитивного мошенничества до высокотехнологичного инструмента кибершпионажа и вымогательства. Если в 2000-е годы атаки были массовыми и неспецифичными, то к 2010-м произошёл переход к целевым кампаниям (spear phishing, whaling), нацеленным на конкретных сотрудников для получения доступа к критическим системам. Современный этап (2020-е) характеризуется полной модернизацией угрозы: распространение сервисов «Фишинг-как-услуга» (PhaaS) и интеграция искусственного интеллекта для генерации безупречных текстов, глубоких фейков и автоматизации разведки. Это радикально снижает порог входа для злоумышленников и повышает эффективность атак, делая традиционные методы фильтрации на основе сигнатур неэффективными.

1.2. Актуальность проблемы целевого фишинга для АСУП в современных российских реалиях

Актуальность разработки специализированной системы защиты от целевого фишинга для АСУП обусловлена совокупностью четырех критических факторов, формирующих уникально сложную среду для российского бизнеса.

1. Высокая интенсивность и приоритетность атак. Россия стабильно входит в число основных целей для киберпреступников. На её долю в 2024-2025 гг. приходилось от 14% до 16% всех успешных кибератак в мире, а прогнозы на 2026 год указывают на возможный рост их числа на 30–35%. Организации, использующие АСУП для управления финансами, производством и логистикой, представляют собой высокоценные мишени.

2. Технологическая эволюция угрозы, усиленная искусственным интеллектом. Современный фишинг перестал быть атакой по шаблону. Использование генеративного ИИ позволяет злоумышленникам в реальном

времени создавать безупречные с точки зрения языка и стиля персонализированные письма, подделывать голосовую и визуальную коммуникацию (дипфейки). Это сводит на нет эффективность традиционных фильтров, ищущих грамматические ошибки, и многократно усиливает психологическое давление на сотрудника.

3. Смещение вектора атак на человеческий фактор и цепочки поставок. По мере усиления технической защиты периметра АСУП основным вектором проникновения становится сотрудник. Злоумышленники атакуют не систему напрямую, а человека, имеющего к ней легитимный доступ, через фишинг и социальную инженерию. Параллельно растет угроза атак через цепочки поставок — компрометация подрядчиков, разработчиков ПО или облачных сервисов, что позволяет обойти защиту самой организации. Защита АСУП больше не ограничивается её техническим контуром.

4. Жесткое нормативно-правовое и экономическое давление. Российские компании, особенно субъекты КИИ, находятся под действием ужесточающегося регулирования (152-ФЗ, 187-ФЗ). В 2025 году введены кратно увеличенные штрафы за утечки персональных данных, которые могут достигать процентов от годового оборота компании. ФСБ России утвердила новые приказы, сокращающие сроки информирования о киберинцидентах до 3 часов для значимых объектов КИИ, что требует от организаций выстроенных и автоматизированных процессов реагирования. Таким образом, последствия успешной фишинговой атаки вышли далеко за рамки прямого ущерба, превратившись в значительный регуляторный и репутационный риск.

1.3. Системный анализ современных киберугроз для АСУП: классификация и взаимосвязи

Проведенный анализ позволяет структурировать угрозы для АСУП, где целевой фишинг выступает не изолированным явлением, а ключевым звеном в цепочке более сложных атак.

Таблица 1.1: Классификация актуальных киберугроз для АСУП и их связь с вектором целевого фишинга

Категория угрозы	Конкретные проявления и тренды (2025-2026 гг.)	Роль целевого фишинга в реализации	Потенциальное воздействие на АСУП
Социальная инженерия и фишинг	– Целевой фишинг (Spear Phishing): Персонализированные атаки на сотрудников с доступом к АСУП. – Фишинг с использованием ИИ: Генерация писем и дипфейков для обмана систем и людей. – BEC (Business Email Compromise): Мошенничество с подменой руководства для санкционирования платежей.	Основной инициирующий вектор. Является самым распространенным методом для получения первоначального доступа к корпоративной сети или учетным данным сотрудника АСУП.	Нарушение конфиденциальности (утечка учетных данных), создание точки входа для последующих атак.

Вредоносное ПО (Malware)	– Многофункциональные трояны: Совмещают функции похитителя данных, шифровальщика и средства удаленного доступа. – Использование легитимных инструментов (Living off the Land): Маскировка под стандартное ПО АСУП.	Ключевой канал доставки. Вредоносное вложение или ссылка в фишинговом письме — стандартный способ инфицирования рабочей станции, с которой осуществляется доступ к АСУП.	Нарушение целостности и доступности данных, кража информации, шифрование данных, долгосрочный контроль над системой.
Атаки на цепочки поставок	– Компрометация подрядчиков, обслуживающих АСУП. – Внедрение уязвимостей в обновления легитимного или импортозамещенного ПО.	Сопутствующий вектор. Фишинг может быть направлен на сотрудников компаний-подрядчиков для получения доступа к их системам и последующей атаки на основную организацию.	Косвенное, но высокоэффективное проникновение в АСУП в обход основных средств защиты, массовые инциденты.

Кибершпионаж и целевые атаки (APT)	– Длительные кампании по хищению интеллектуальной собственности, данных НИОКР, финансовой отчетности. – Атаки на объекты критической инфраструктуры (ОПК, энергетика).	Стандартный вектор начального доступа. Для APT-групп фишинг — это наиболее надежный и незаметный способ проникновения в изолированную среду и получения учетных данных привилегированных пользователей.	Критическое нарушение конфиденциальности, хищение коммерческой тайны, нанесение ущерба экономической и технологической безопасности.

1.4. Психологические механизмы и модель уязвимости сотрудника в АСУП

Успех фишинга основан на эксплуатации универсальных паттернов мышления. Используя принципы влияния Роберта Чалдини (авторитет, срочность, социальное доказательство), атакующие создают непреодолимое для сознания давление. В контексте АСУП наиболее опасен принцип авторитета — фишинговое письмо, имитирующее указание руководителя, вынуждает сотрудника обойти внутренние регламенты для быстрого выполнения «задачи». Ключевым выводом для проектирования защиты является понимание, что уязвимость сотрудника - это не константа, а переменная, зависящая от индивидуальных, контекстуальных (стресс, усталость) и технологических факторов (качество подделки). Это требует перехода от разового обучения к непрерывному адаптивному циклу тренингов, моделирующему реальное давление, что и будет заложено в основу предлагаемой методики.

1.5. Технический арсенал современного целевого фишинга

Эффективность атак обеспечивается сочетанием социальной инженерии и постоянно эволюционирующего технического инструментария. Помимо классического спуфинга доменов, злоумышленники активно используют:

1. Сложную обфускацию: Размещение фишинг-ландшафтов на легитимных скомпрометированных ресурсах (облачные хранилища, GitHub Pages) для обхода чёрных списков.
2. Атаки типа Adversary-in-the-Middle (AitM): Проксирование сессий жертвы для обхода многофакторной аутентификации (MFA) - одной из ключевых технических контрмер.
3. Использование легитимных инструментов: Доставка вредоносной нагрузки через документы Office с эксплойтами или скрипты (например, VBA), что затрудняет обнаружение.

Данный анализ напрямую определяет требования к техническому контуру защиты в рамках методики: необходимость не просто MFA, а её устойчивых реализаций, а также использование песочниц и поведенческого анализа для обнаружения сложных угроз.

1.6. Экономика фишинга и нормативно-правовой контекст в РФ

Ущерб от успешной атаки носит комплексный характер. Помимо прямых финансовых потерь (выкуп, хищение средств), компания сталкивается с затратами на ликвидацию инцидента, колоссальным репутационным ущербом и риском многомиллионных штрафов по статьям 152-ФЗ «О персональных данных» и 187-ФЗ «О безопасности КИИ». Экономический расчёт, проведённый в разделе 3.4, наглядно показывает, что инвестиции в превентивную систему защиты на порядок окупаются за счёт предотвращённого ущерба. Таким образом, построение системы защиты трансформируется из рекомендации в обязательное условие операционной и финансовой устойчивости бизнеса в российских реалиях.

1.7. Сравнительный анализ существующих стандартов и выявление «слепых зон»

Несмотря на обилие стандартов ИБ, ни один из них не предлагает целостной методики, специально сфокусированной на противодействии целевому фишингу в среде АСУП. Сравнительный анализ ключевых стандартов позволяет выявить их системные ограничения.

Таблица 1.2: Сравнительный анализ стандартов ИБ в контексте защиты АСУП от целевого фишинга

Критерий / Стандарт	NIST Cybersecurity Framework (CSF) & SP 800-53	ISO/IEC 27001:2022	СТО БР ИББС-1.0-2014
Фокус на человеческий фактор	Контроли «Awareness and Training» есть, но без специфики фишинга.	Требует обучения, но методы и контент оставляет на откуп организации.	Включает требования к обучению, но в рамках отраслевой специфики банков.
Учёт специфики АСУП	Косвенный, через общие контроли для систем. Прямой привязки к бизнес-процессам АСУП нет.	Отсутствует. Защита АСУП должна быть выведена организацией из общего анализа рисков.	Высокий. Специально для банковских (автоматизированных) систем, что является ближайшим аналогом.

Пригодность для оперативной адаптации	Задаёт цикл управления рисками, но не содержит механизмов быстрой корректировки мер под новые тактики фишинга.	Цикл PDCA есть, но его наполнение зависит от скорости реакции самой организации.	Содержит цикл PDCA, но может быть излишне формализован для гибкого реагирования.
Ключевой недостаток для нашей задачи	Высокая общность и объём. Сложно выделить приоритетные контроли именно против фишинга для АСУП.	Избыточная гибкость. Не отвечает на вопрос «как именно», не предоставляет готовых решений.	Отраслевая ограниченность. Требует адаптации для АСУП небанковских предприятий.

Критический анализ позволяет выявить ключевую «слепую зону»: существующие подходы не предлагают ролево-ориентированной модели, где оценка риска и набор контрмер для сотрудника напрямую зависят от его доступа к конкретным модулям и данным АСУП (финансы, ПДн, коммерческая тайна). Этот пробел и призвана заполнить разрабатываемая методика.

1.8 Выводы по первой главе

Проведённый анализ однозначно свидетельствует, что целевой фишинг представляет собой комплексную гибридную угрозу, борьба с которой требует выхода за рамки традиционных, фрагментарных подходов. Существующие международные и отраслевые стандарты, выполняя важную функцию формирования общего поля ИБ, не предоставляют специализированного, готового к применению инструментария для защиты именно АСУП. Их основные недостатки — отсутствие глубокой интеграции с бизнес-процессами АСУП, ролевой оценки уязвимостей и встроенного цикла оперативной адаптации на основе измеримых метрик.

Таким образом, сформирована чёткая научно-практическая проблема: существует объективная необходимость в разработке специализированной методики защиты информации от целевого фишинга, которая, синтезируя процессный подход стандартов, преодолеет их «слепые зоны» за счёт ролевой модели рисков, интеграции с АСУП и замкнутого цикла адаптивного управления. Решению данной проблемы и посвящена следующая глава данной работы.

ГЛАВА 2. РАЗРАБОТКА МЕТОДИКИ ЗАЩИТЫ ОТ ЦЕЛЕВОГО ФИШИНГА ДЛЯ АСУП

2.1. Методологическая основа и принципы построения методики защиты

Логика раздела: Перейти от анализа угроз (Глава 1) к конструктивному этапу. Определить концептуальный каркас (методологии) и базовые правила (принципы), на которых будет строиться вся последующая методика. Это обеспечит ее системность, воспроизводимость и соответствие лучшим практикам.

2.1.1. Выбор и адаптация базовых методологий

Проектирование методики требует опоры на признанные управленческие и отраслевые подходы. Для противодействия целевым фишинговым атакам наиболее уместны следующие методологии, объединенные в единый каркас:

1. Процессный подход PDCA (Plan-Do-Check-Act): Этот циклический метод лежит в основе многих международных и национальных стандартов, включая ГОСТ Р ИСО/МЭК 27001, и обеспечивает непрерывное совершенствование системы защиты. Применительно к нашей методике:

- Планирование (Plan): Этапы оценки рисков и проектирования контрмер (разделы 2.2, 2.3, 2.4).
- Внедрение (Do): Практическая реализация и апробация (Глава 3).
- Проверка (Check): Мониторинг эффективности, анализ инцидентов, учебные фишинг-тесты (встроено в процессы 2.3, 2.5).
- Действие (Act): Корректировка методики на основе полученных данных.

2. Управление рисками (ГОСТ Р ИСО/МЭК 27005): Угроза целевого фишинга должна управляться через призму рисков. Методика интегрирует классический процесс риск-менеджмента:

- Идентификация активов, угроз и уязвимостей (на основе данных Главы 1).
- Анализ и оценка рисков (раздел 2.2).
- Выбор и внедрение мер обработки рисков (разделы 2.3, 2.4).

- Мониторинг и пересмотр рисков (разделы 2.5, 2.6).

3. Тактико-технические модели (MITRE ATT&CK, Kill Chain): Для обеспечения адекватности защиты инструментарию злоумышленника (анализ 1.5) методика использует эти фреймворки как таксономию угроз. Они позволяют детализировать этапы фишинговой атаки (от разведки до целевых действий) и выстраивать контрмеры для срыва атаки на каждом этапе.

2.1.2. Принципы построения методики защиты для АСУП

Исходя из специфики АСУП как критически важной, сложной информационной системы и природы целевого фишинга, методика формулируется на основе следующих ключевых принципов:

- Принцип комплексности и эшелонированности: Защита должна включать взаимодополняющие организационные, технические и кадровые меры, перекрывающие все этапы возможной атаки (от профилактики до реагирования).
- Принцип непрерывности и адаптивности: Противодействие фишингу — не разовое мероприятие, а непрерывный цикл (PDCA), адаптирующийся к эволюции угроз и изменениям в самой АСУП.
- Принцип централизованного управления и децентрализованного исполнения: Общая политика и координация исходят от службы ИБ (центр), но конкретные меры (например, соблюдение регламентов) реализуются на уровне пользователей и администраторов АСУП (децентрализация).
- Принцип ролевой и риск-ориентированной направленности: Интенсивность и тип защитных мер должны быть пропорциональны уровню риска, связанного с конкретной ролью пользователя в АСУП (бухгалтер, системный администратор и т.д.).
- Принцип минимальных привилегий и необходимости: Каждый пользователь АСУП должен обладать только теми правами доступа, которые абсолютно необходимы для выполнения его трудовых функций. Это ограничивает потенциальный ущерб от успешного фишинга.
- Принцип экономической обоснованности: Затраты на реализацию методики не должны превышать вероятный ущерб от успешной атаки. Данный

принцип обеспечивает практическую реализуемость методики и требует проведения расчетов.

2.1.3. Архитектура методики как единого механизма

Методика представляет собой целостный механизм, объединяющий методологии и принципы в логическую последовательность этапов. Ее архитектуру можно визуализировать в виде замкнутого цикла, интегрированного в жизненный цикл АСУП.

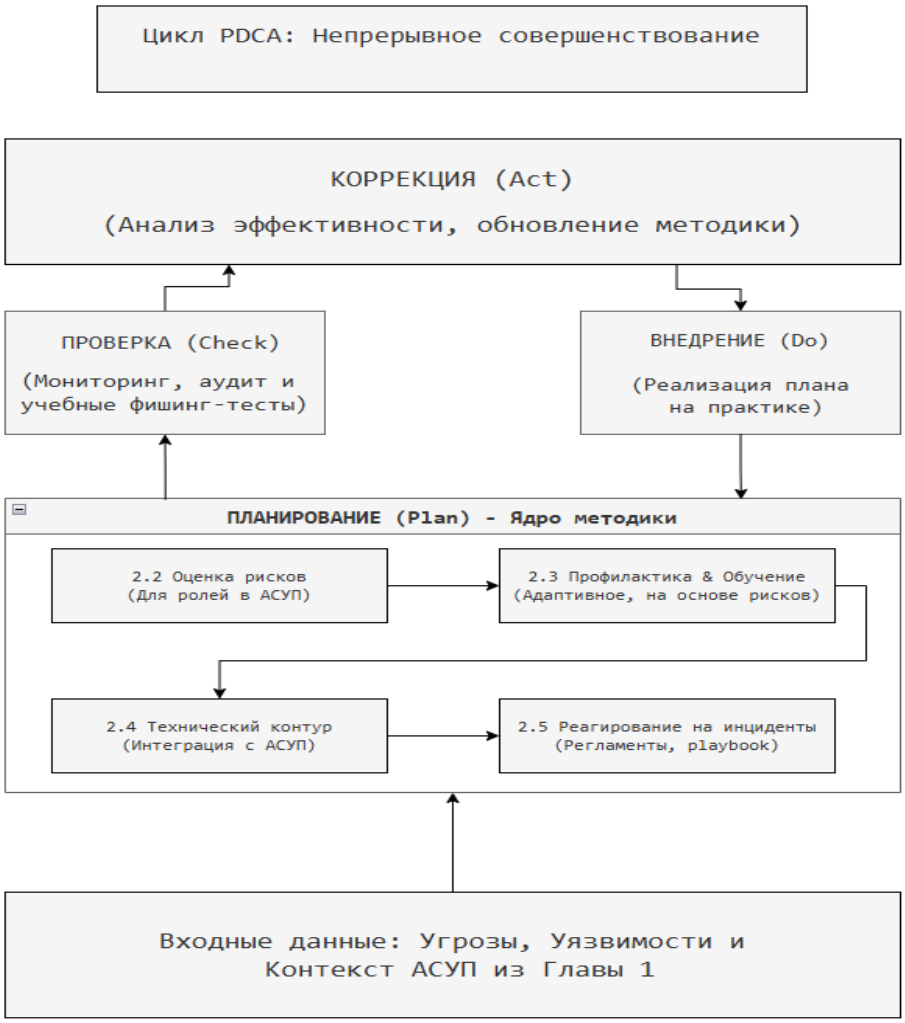

Рисунок 2.1. Схема высокоуровневой архитектуры методики защиты от целевого фишинга в АСУП

2.2. Разработка модели оценки рисков целевого фишинга для ролей в АСУП

Этот раздел посвящён созданию ядра методики - адаптированной формулы риска, позволяющей вычислять уровень угрозы для каждой роли в АСУП. Модель строится на трёх ключевых факторах, выявленных в Главе 1: ценность актива, угроза и уязвимость.

2.2.1. Обоснование и структура модели

Традиционная формула риска (Риск = Угроза × Уязвимость × Ущерб) адаптируется под специфику целевого фишинга и корпоративного контекста: Риск_роли = (Ценность_доступа_роли) × (Вероятность_атаки_на_роль) × (Коэффициент_уязвимости_роли)

Эта модель обеспечивает объективное, сравнимое численное значение для каждой должности, что позволяет службе ИБ обоснованно распределять ресурсы.

2.2.2. Детализация компонентов модели и методика их оценки

Для применения модели каждый компонент нуждается в чёткой параметризации.

1. Ценность доступа роли (Ц) Определяет потенциальный ущерб от компрометации учётной записи. Оценивается по шкале от 1 до 5 путём анализа уровня привилегий роли в АСУП:

- 5 (Критический): Доступ к финансовым модулям, мастер-данным, управлению системами.
- 3 (Высокий): Доступ к конфиденциальным проектным данным, персональным данным сотрудников.
- 1 (Низкий): Доступ только к общедоступной внутренней информации.

2. Вероятность атаки на роль (В) Отражает степень «привлекательности» роли для злоумышленника. Оценивается от 1 до 5 на основе:

- Данные отраслевой статистики: Например, данные о том, что 43% успешных атак используют социальную инженерию, а государственный и промышленный сектора — ключевые цели.
- Результаты пассивной разведки: Роли, чьи контакты и должностные функции легко обнаружить в открытых источниках (LinkedIn, корпоративный сайт), получают более высокий балл.

- Вовлечённость во внешние коммуникации: Сотрудники, активно работающие с контрагентами (например, отдел закупок), более подвержены атакам с подменой лиц (BEC).

3. Коэффициент уязвимости роли (У) Измеряет устойчивость конкретного сотрудника к фишингу. Динамический параметр, рассчитываемый по формуле: У = (Базовый_коэффициент) – (Эффективность_обучения_и_тестов)

- Базовый коэффициент (макс. 5) определяется историей инцидентов и результатами первичного тестирования.
- Эффективность обучения — снижающая корректировка (от 0 до 2 баллов) на основе регулярных метрик: процент успешных учебных фишинг-атак, скорость сообщения об инцидентах.

2.2.3. Практическое применение модели: пример расчёта и визуализация

Рассмотрим применение модели для трех гипотетических ролей в АСУП производственного предприятия.

Роль в АСУП	Ценность доступа (Ц)	Вероятность атаки (В)	Коэф. уязвимости (У)	Итоговый риск (Ц × В × У)
Главный бухгалтер (Доступ к фин. модулям, зарплате)	5	5 (ключевая цель для BEC)	4 (базовый) – 1 (обучение) = 3	5 × 5 × 3 = 75
Инженер-технолог (Доступ к чертежам и спецификациям)	4	4 (цель для пром. шпионажа)	5 (базовый) – 0.5 = 4.5	4 × 4 × 4.5 = 72

Сотрудник отдела кадров (Доступ к базе ПДн сотрудников)	4	3	4 (базовый) – 1.5 = 2.5	4 × 3 × 2.5 = 30

Интерпретация результата: Модель количественно показывает, что риски для главного бухгалтера и инженера-технолога сопоставимы и критически высоки, однако природа угрозы разная (финансовая vs. шпионаж). Это требует разных приоритетов в защите: для первой роли - усиление процедур подтверждения транзакций, для второй - мониторинг утечек данных. Риск для отдела кадров - умеренный.

2.2.4. Интеграция модели в цикл управления безопасностью

Данная модель - не разовый инструмент, а часть процесса PDCA (Plan-Do-Check-Act):

1. Plan: Матрица рисков используется для планирования адаптивных программ обучения (раздел 2.3) и настройки технических контрмер (раздел 2.4).
2. Do/Check: Результаты учебных фишинг-тестов и мониторинга инцидентов проверяются и используются для корректировки коэффициента уязвимости (У).
3. Act: Цикл пересчёта рисков запускается регулярно (например, ежеквартально) или после значимых изменений, обеспечивая адаптивность методики.

2.3. Проектирование ключевых процессов методики: профилактика и обучение

Данный раздел посвящен разработке центрального элемента системы защиты от целевого фишинга — адаптивной программы обучения (Security Awareness) и профилактических процедур. Основываясь на матрице рисков, полученной в разделе 2.2, мы переходим от оценки к действию, проектируя непрерывный процесс, направленный на минимизацию ключевой уязвимости — человеческого фактора.

2.3.1. Принципы проектирования адаптивной обучающей программы

Эффективная программа строится не на разовых лекциях, а на фундаментальных принципах, доказавших свою результативность в противодействии современным угрозам:

1. Риск-ориентированность и персонализация: Содержание, сложность и частота обучения напрямую зависят от уровня риска, присвоенного роли в АСУП (раздел 2.2). Для высокорисковых ролей (главный бухгалтер, системный администратор) сценарии имитируют целевой фишинг (spear phishing) и китобойный промысел (whaling), а обучение проводится чаще.

2. Непрерывность и регулярность: Навыки распознавания фишинга деградируют без практики. Исследования показывают, что эффект от единичных тренингов статистически незначим. Программа должна представлять собой непрерывный цикл с регулярными активностями (ежемесячные микровоздействия, квартальные углубленные курсы).

3. Практико-ориентированность: Теория закрепляется через иммерсивную практику. Ключевой инструмент — регулярные фишинг-симуляции, максимально приближенные к реальным рабочим ситуациям и каналам коммуникации (email, мессенджеры).

4. Позитивное подкрепление: Цель — создать культуру открытости, а не страх. Сотрудники, сообщившие о подозрительном письме, поощряются. Акцент делается на обучении на ошибках, а не на наказании.

2.3.2. Алгоритм формирования и контент обучающих программ

На основе матрицы рисков для каждой категории ролей формируется индивидуальный учебный план. Пример увязки риска и форматов обучения:

Уровень риска (из раздела 2.2)	Целевые роли в АСУП	Частота фишинг-симуляций	Ключевые темы и форматы обучения

Критический (70-100)	Руководители, гл. бухгалтеры, админы	1 раз в 2-3 недели	Whaling/BEC: Симуляции от имени «вышестоящего руководства» с запросом конфиденциальных данных или финансовой операции. Мини-курсы по процедурам двойного подтверждения.
Высокий (40-69)	Инженеры, специалисты по закупкам, HR	1 раз в месяц	Целевой фишинг: Персонализированные сценарии, связанные с профессиональной деятельностью (запрос чертежей, данных сотрудников). Курсы по защите конфиденциальной информации и работе с ПДн.
Средний (20-39)	Офис-менеджеры, рядовые специалисты	1 раз в квартал	Массовый и социальный фишинг: Распознавание общих признаков мошенничества, безопасная работа с почтой, создание надежных паролей.

Содержательное ядро программы составляют интерактивные модули, покрывающие:

- Основы ИБ и работа с конфиденциальной информацией.
- Психология и методы социальной инженерии.
- Анализ фишинговых писем и сайтов (с интерактивными заданиями).
- Безопасность паролей и удаленной работы.

2.3.3. Методика проведения фишинг-симуляций и анализа результатов

Фишинг-симуляция — главный инструмент для оценки и повышения устойчивости персонала. Ее проведение регламентируется следующим алгоритмом:

Рисунок 2.3.1 - схема цикла проведения учебной фишинг-атаки и обучения

Для измерения эффективности используются поведенческие метрики, а не тесты на знание теории:

1. Уровень подверженности фишингу (Phish-prone rate) (%): Доля сотрудников, выполнивших опасное действие (клик по ссылке, открытие вложения). Мировой эталон для зрелой программы — около 4%.

2. Время до первого сообщения о фишинге (Time to first report) (мин.): Время от начала симуляции до первого сообщения в ИБ-службу. Показатель сформированной культуры безопасности.

3. Показатель сообщений о фишинге (Report rate) (%): Доля сотрудников, сообщивших об атаке. Целевой показатель — более 50%.

4. Коэффициент снижения риска: Динамика изменения уровня подверженности фишингу за период (например, полгода). Регулярное обучение может снизить количество инцидентов в 15-20 раз.

2.3.4. Разработка организационных регламентов и памяток

Обучение подкрепляется формальными процедурами, интегрированными в бизнес-процессы АСУП:

1. Регламент подтверждения критичных действий: для операций с высоким риском (перевод средств, выгрузка баз данных) вводится обязательное подтверждение по альтернативному, независимому каналу (например, устное по телефону).

2. Памятка-чек-лист для сотрудника: Одностраничный гайд с алгоритмом проверки подозрительного письма: отправитель, ссылки, вложения, чувство срочности. Интегрируется в корпоративный портал или как плакат.

3. Процедура информирования ИБ-службы: Простой и гарантированный способ (специальный адрес email, кнопка в почтовом клиенте) для быстрого сообщения об инциденте без страха санкций.

2.4. Проектирование технического контура защиты в среде АСУП

Данный раздел посвящен разработке технической архитектуры, предназначенной для автоматизации обнаружения, блокировки и минимизации последствий целевых фишинговых атак, направленных на АСУП. Основываясь на оценке рисков (раздел 2.2) и учитывая особенности поведения пользователей (раздел 2.3), проектируемый контур создает многоуровневый эшелон обороны. Его цель — интегрировать современные средства защиты в процессы работы АСУП, обеспечивая как превентивное противодействие угрозам, так и оперативное реагирование на инциденты.

Ключевой принцип: Комплексный подход, объединяющий технические средства, обучение персонала и организационные процедуры, является наиболее

эффективным способом борьбы с фишингом. Технический контур выступает основой, усиленной осведомленными пользователями и четкими регламентами.

2.4.1. Модель интеграции и архитектура защитного контура

Технический контур защиты от фишинга для АСУП строится по принципу «глубокой эшелонированной обороны» (Defense in Depth). Его архитектура включает несколько последовательных и взаимодополняющих слоев, интегрированных в корпоративную ИТ-инфраструктуру.

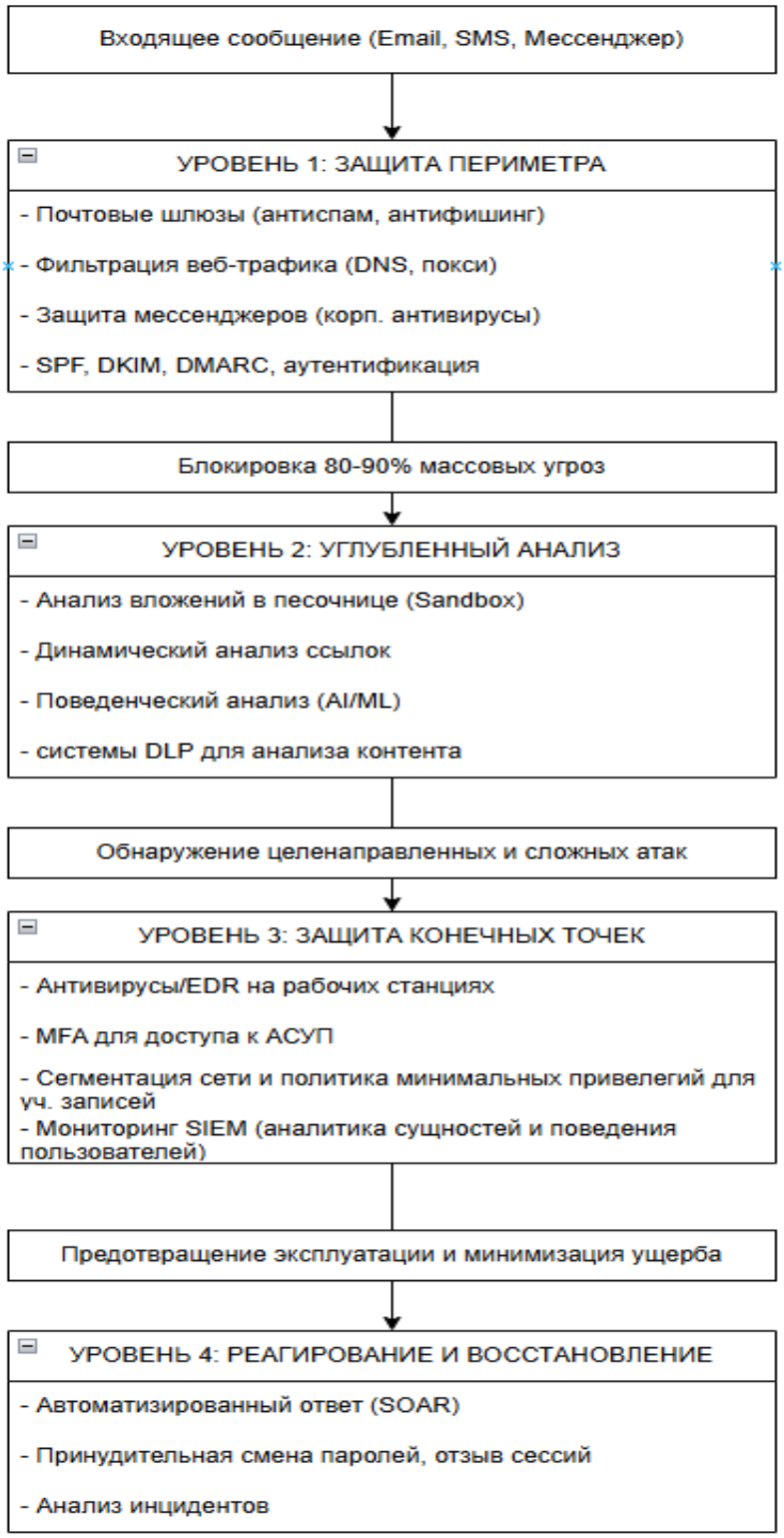

Рисунок 2.4.1 - Схема многоуровневой архитектуры технического контура защиты от фишинга

2.4.2. Детализация ключевых технических средств и их настройка для АСУП

Для каждого уровня защиты требуются конкретные решения, настраиваемые с учетом специфики защищаемых данных и бизнес-процессов АСУП.

1. Периметрическая защита и аутентификация электронной почты

- Современные почтовые шлюзы должны выходить за рамки статической сигнатурной проверки. Критически важны функции машинного обучения для анализа стилистики письма, метаданных и выявления аномалий, характерных для целевого фишинга. Шлюз должен «понимать» содержание, распознавать текст на изображениях и оценивать репутацию отправителей.
- Обязательная реализация стандартов аутентификации для корпоративного домена является базовым требованием:
  - SPF (Sender Policy Framework): Определяет перечень серверов, имеющих право отправлять почту от имени домена компании.
  - DKIM (DomainKeys Identified Mail): Добавляет к исходящим письмам криптографическую подпись, гарантирующую их целостность и подлинность.
  - DMARC (Domain-based Message Authentication, Reporting & Conformance): Политика, указывающая получателям, как обрабатывать письма, не прошедшие проверки SPF/DKIM (отклонять, помещать в спам), и предоставляющая детальную отчетность о всех попытках отправки. Внедрение DMARC с политикой reject для внешних получателей — одна из самых эффективных мер против спуфинга домена.

2. Углубленный анализ контента с использованием DLP и песочниц

- DLP-системы (Data Loss Prevention) выполняют роль «последнего рубежа» для пропущенных фишинговых писем. Их можно настроить на автоматический поиск инцидентов по гибким политикам:

- Поиск ключевых фраз, характерных для фишинга («срочно авторизуйтесь», «ваша учетная запись будет заблокирована», «необходимо оплатить»).
- Обнаружение замаскированных ссылок (bit.ly, tinyurl) и подозрительных доменов (например, rnicrosoft.com вместо microsoft.com) с помощью регулярных выражений.
- Выявление опасных вложений по расширениям (.exe, .js, .scr, .iso) и их хеш-суммам.

- Песочницы (Sandboxing) критически важны для анализа вложений и ссылок в изолированной среде. Современные решения эмулируют различные ОС и приложения, отслеживая поведение потенциально вредоносного кода и блокируя угрозу до её попадания к пользователю.

3. Защита конечных точек и доступ к АСУП

- Многофакторная аутентификация (MFA) является обязательной для всех учетных записей с доступом к АСУП, особенно для привилегированных пользователей. MFA радикально снижает риски даже в случае компрометации логина и пароля через фишинг.
- Принцип наименьших привилегий и сегментация сети. Пользовательские учетные записи в АСУП должны иметь строго необходимый для работы уровень доступа. Сеть должна быть сегментирована таким образом, чтобы компрометация рабочей станции в одной зоне не давала прямого доступа к серверам АСУП с критичными данными.

2.4.3. Организационно-технические процедуры и интеграция с процессами

Технические средства эффективны только при поддержке четких организационных процедур.

- Регламент проверки и удаления фишинговых писем. На основе алертов от DLP или сообщений пользователей ИБ-специалист должен иметь возможность в течение 10-15 минут инициировать удаление вредоносного письма с почтовых ящиков всех сотрудников через запрос в ИТ-отдел.

- Анализ воздействия с помощью DLP. При успешной атаке система DLP позволяет построить «контентный маршрут»: отследить, сколько пользователей получили письмо, кто открыл вложение или перешел по ссылке, оценить потенциальный ущерб.
- Интеграция с SOC (Security Operations Center). События от всех уровней защиты (шлюзы, DLP, EDR, MFA) должны агрегироваться в системе SIEM. Это позволяет выстраивать корреляционные правила для обнаружения сложных многоэтапных атак (например, «фишинговое письмо -> переход по ссылке -> аномальная активность в АСУП») и обеспечивать оперативное реагирование.

2.4.4. Сравнительный анализ и критерии выбора программных продуктов

Выбор конкретных технических средств для реализации спроектированного контура защиты является критически важным этапом. Он должен основываться не только на заявленных возможностях вендоров, но и на строгих критериях, вытекающих из модели угроз (Глава 1), архитектуры защиты и специфики АСУП. Ниже представлен сравнительный анализ релевантных категорий программных решений для защиты от целевого фишинга.

Таблица 2.4.1: Сравнительный анализ программных решений для защиты от целевого фишинга в среде АСУП

Категория решения	Примеры продуктов	Ключевые функции и технологии (на основе анализа продуктов)	Преимущества для АСУП	Рекомендуемые сценарии применения

Специализированные почтовые шлюзы (SEG)	AVSoft KAIROS, Mimecast, Barracuda Email Protection	Многоуровневая проверка (сессия, заголовки, репутация). Глубокий анализ ссылок (статический, динамический, JS-код) и вложений. Машинное обучение для анализа текста и изображений. Строгое применение SPF, DKIM, DMARC. Интеграция с песочницей (Sandbox).	Комплексная фильтрация всего входящего почтового трафика — основного вектора атак. Высокая точность детектирования за счет ИИ. Защита от спуфинга домена компании. AVSoft KAIROS внесен в Реестр российского ПО, что критично для многих АСУП.	Базовый и обязательный элемент контура для любой организации. AVSoft KAIROS особенно актуален для компаний, ориентированных на импортозамещение или работающих с гостайной.

Решения на базе API (облачная безопасность)	Microsoft Defender для Office 365, Avanan, Abnormal Security	Глубокая интеграция с облачными почтовыми платформами (Microsoft 365, Google Workspace). Поведенческий анализ и построение графа отношений между сотрудниками для выявления BEC. Безопасные ссылки (Safe Links) и вложения. Автоматическое устранение угроз.	Бесшовная работа в родной экосистеме. Обнаружение сложных атак, не имеющих вредоносных ссылок или вложений (чистый BEC). Высокая скорость развертывания и обновлений.	Организации, полностью перешедшие на Microsoft 365/Google Workspace. Идеальное дополнение к нативным возможностям платформ для защиты от целевых атак.

Платформы аутентификации электронной почты	PowerDMARC	Специализация на настройке и мониторинге политик DMARC, SPF, DKIM. Анализ угроз на основе отчетов DMARC. Помощь в достижении строгой политики p=reject.	Максимальное снижение риска спуфинга домена компании. Не защищает от фишинга с легитимных, но взломанных ящиков.	Критически важное дополнение для защиты репутации домена АСУП. Обязательно к внедрению после настройки почтового шлюза.
Комплексные платформы безопасности (XDR/ SIEM)	Microsoft Defender XDR, IRONSCALES	Корреляция событий с почты, конечных точек, идентификаций. Расширенное обнаружение и реагирование (XDR). Интеграция с обучением	Позволяет выявлять не изолированные фишинговые письма, а цепочки атак (письмо → клик → вредоносная активность в АСУП). Централизованное реагирование.	Для зрелых SOC (Центров мониторинга и реагирования). Повышает эффективность контура за счет интеграции разрозненных данных.

		(симуляции фишинга).		

Ключевые критерии выбора для среды АСУП

При выборе и комбинации решений из таблицы для конкретной АСУП необходимо оценить их по следующим критериям, разработанным в предыдущих разделах:

1. Соответствие требованиям регуляторов (для РФ): Приоритет решениям из Реестра российского ПО (как AVSoft KAIROS), поддержка необходимых протоколов и возможность ведения аудиторских логов.
2. Глубина анализа контента: Способность анализировать не только текст, но и изображения (логотипы, QR-коды), скрипты на веб-страницах и поведенческие аномалии в тексте писем.
3. Интегрируемость: Наличие API для обмена индикаторами компрометации (IoC) с другими элементами контура (например, SIEM или межсетевыми экранами), что соответствует принципу многоуровневой защиты.
4. Адаптивность: Использование технологий машинного обучения (ИИ), способных дообучаться на специфичном для организации трафике, что критично для противодействия эволюционирующим целевым атакам.

Вывод для пункта 2.4: Внедрение технического контура не сводится к закупке любого антифишингового решения. Это осознанный выбор комбинации продуктов, который должен быть сделан на основе их функционального соответствия выделенным уровням защиты (периметр → анализ → доступ →

реагирование) и конкретным требованиям бизнес-процессов, реализованных в АСУП. Представленная таблица служит основой для такого выбора.

2.5. Разработка регламентов реагирования на инциденты целевого фишинга

Данный раздел посвящен созданию организационного механизма, завершающего цикл управления безопасностью АСУП, — системы оперативного реагирования на инциденты. Если профилактика и техническая защита направлены на предотвращение атаки, то регламенты реагирования определяют порядок действий в случае её успеха. Их цель — минимизировать ущерб, восстановить нормальное функционирование системы и предотвратить повторение аналогичных инцидентов.

Ключевой принцип: Скорость и слаженность действий команды реагирования напрямую влияют на масштаб финансовых, операционных и репутационных потерь. Четкие регламенты превращают хаотичную реакцию в управляемый процесс.

2.5.1. Принципы и структура системы реагирования на инциденты ИБ

Эффективная система строится на фундаменте из нескольких ключевых принципов, согласованных с лучшими практиками и стандартами:

1. Конфиденциальность и ограничение распространения информации: Работа по инциденту ведется в закрытом режиме, чтобы избежать паники, не спровоцировать злоумышленника и не усложнить расследование.

2. Оперативность и эскалация: Каждый инцидент имеет установленные сроки реакции и цепочку эскалации в зависимости от критичности.

3. Документированность: Все этапы работы, принятые решения и найденные артефакты фиксируются в журнале инцидента для последующего анализа и возможных юридических нужд.

4. Целостность доказательств: Работа с компрометированными системами ведется таким образом, чтобы сохранить цифровые следы для расследования, избегая их модификации.

2.5.2. Классификация инцидентов целевого фишинга и матрица реагирования

Не все инциденты равнозначны. Для эффективного распределения ресурсов они классифицируются по степени серьезности на основе модели рисков из раздела 2.2 и потенциального воздействия на бизнес-процессы АСУП.

Уровень	Критерии классификации	Пример сценария	Целевое время реакции	Ответственный
Критический (Уровень 1)	Компрометация учетной записи привилегированного пользователя (администратор АСУП, CFO). Фактическая или попытка финансовой операции через ВЕС. Установка вредоносного ПО (шифровальщик, бэкдор).	Бухгалтер перешел по фишинговой ссылке, ввел учетные данные для доступа к банк-клиенту.	Немедленно (в течение 15 мин.)	ЦИР (CIRT), руководство. Требуется мобилизация всей команды.
Высокий (Уровень 2)	Компрометация учетной записи сотрудника с доступом к конфиденциальным данным АСУП (ПДн, КИ). Успешная передача данных	Сотрудник отдела кадров отправил выписку по персоналу на внешний адрес, поверив письму от	В течение 1 часа	Ведущий аналитик ИБ. Эскалация на руководство.

	по фишинговому запросу.	"руководства".		
Средний (Уровень 3)	Клик по фишинговой ссылке или открытие вложения сотрудником из группы риска. Попытка фишинга, заблокированная на периметре, но требующая анализа.	Инженер кликнул на ссылку в письме от "поставщика", но система MFA заблокировала вход.	В течение 4 часов	Аналитик ИБ. Стандартная процедура по playbook.
Низкий (Уровень 4)	Получение сотрудником подозрительного письма и его корректное информирование службы ИБ. Массовый фишинг, не прошедший фильтры.	Сотрудник прислал в ИБ-службу скриншот письма с явными признаками мошенничества.	В течение 1 рабочего дня	Специалист ИБ первой линии. Регистрация и блокировка угрозы.

2.5.3. Регламент (Playbook) реагирования на инцидент с компрометацией учетной записи

Для наиболее типового и опасного сценария — компрометации учетных данных через фишинг — разрабатывается детальный пошаговый алгоритм (playbook). Это инструкция для команды SOC/ЦИР.

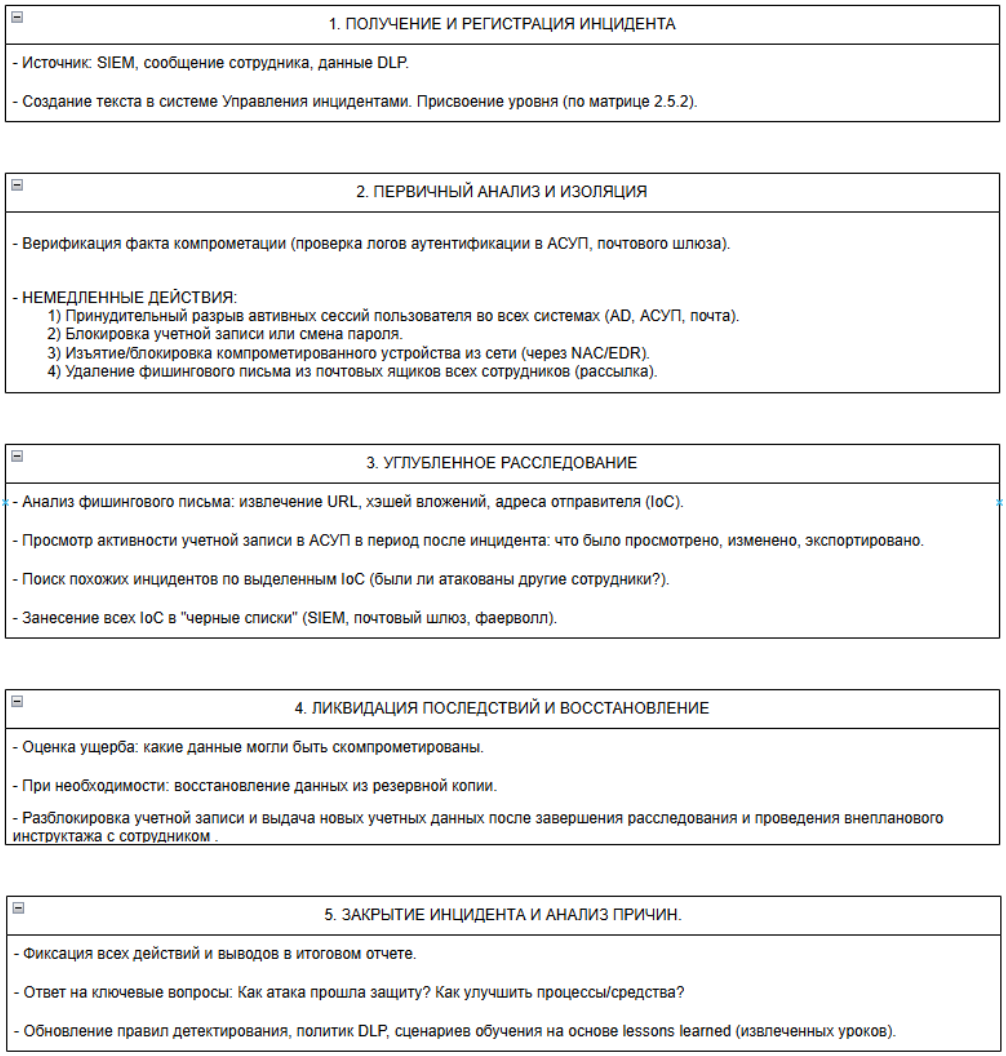

Рисунок 2.5.1 - Регламент реагирования на инцидент "Компрометация учетной записи через фишинг"

2.5.4. Ролевая модель и шаблоны документирования

Для реализации регламентов необходима четкая ответственность и инструменты фиксации информации.

- Ролевая модель: Определяются ответственные за каждый этап: Специалист 1-й линии поддержки (прием заявок), Аналитик SOC (расследование), Инженер ИБ (технические действия), Руководитель (эскалация, связь с руководством).

- Шаблон журнала инцидента: Единая форма для фиксации: время, описание, уровень, статус, выполненные действия, извлеченные IoC, ответственные.
- Шаблон итогового отчета: Структура для анализа: хронология, воздействие на бизнес, коренная причина, рекомендации по предотвращению.

2.6. Научно-техническое и экономическое обоснование методики

Данный раздел завершает проектно-расчетную часть работы, предоставляя количественную и качественную оценку эффективности, реализуемости и экономической целесообразности разработанной методики. Его цель — доказать, что предлагаемый комплекс мер не просто технически корректен, но и является оптимальным решением с точки зрения управления рисками и ресурсами предприятия.

Ключевой принцип: Инвестиции в информационную безопасность должны рассматриваться как стратегические, а их эффективность — поддаваться измерению и обоснованию. Данный раздел отвечает на вопрос руководства: «Почему мы должны внедрить именно эту систему и какую отдачу она принесет?».

2.6.1. Сравнительный анализ с типовыми подходами к защите

Для объективной оценки преимуществ проводится сравнение разработанной методики с наиболее распространенными на практике подходами, выявленными в ходе анализа (Глава 1). Критерии выбраны исходя из требований к современной системе защиты.

Таблица 2.6.1: Сравнительный анализ подходов к защите от целевого фишинга

Критерий	Разрозненные технические меры (Антиспам, АВ)	Разовые тренинги персонала	Предлагаемая комплексная методика

Охват угроз	Узкий, эффективен против массовых атак. Бессилен против персонализированного фишинга и BEC.	Теоретический, не формирует устойчивых навыков против сложных сценариев.	Широкий. Сочетает технические, организационные и человеческие меры, покрывая все этапы атаки.
Адаптивность	Низкая. Требует ручного обновления сигнатур и правил.	Отсутствует. Знания быстро устаревают.	Высокая. Цикл PDCA и модель рисков обеспечивают регулярный пересмотр и актуализацию мер.
Измеримость эффективности	Косвенная (статистика спама). Не измеряет успешность целевых атак.	Субъективная (результаты тестов). Не отражает поведение в реальной ситуации.	Прямая и количественная. Использует матрицу рисков, метрики обучения (Phish-Prone Rate), экономические показатели (ROSI).
Интеграция с АСУП	Фрагментарная. Часто не учитывает бизнес-контекст и критичность данных в системе.	Отсутствует.	Глубокая. Модель рисков построена на ролях и активах АСУП, технический контур интегрирован в процессы.

Соответствие требованиям регуляторов (152-ФЗ, 187-ФЗ)	Частичное. Выполняются лишь технические требования.	Недостаточное. Нет документально подтвержденного цикла обучения.	Полное. Методика формирует доказательную базу (политики, регламенты, журналы инцидентов, отчеты об обучении).
Основной недостаток	Создает ложное чувство безопасности, оставляя «слепые зоны».	Не меняет корпоративную культуру безопасности.	Требует первоначальных инвестиций и междисциплинарного управления.

Вывод по анализу: Предлагаемая методика преодолевает ключевой недостаток традиционных подходов — их разрозненность. Она представляет собой не набор инструментов, а целостную систему управления риском фишинга, что является необходимым условием в условиях современных угроз.

2.6.2. Модель расчёта экономической эффективности (ROSI)

Для обоснования инвестиций используется адаптированная модель Return on Security Investment (ROSI) — Возврат на инвестиции в безопасность.

1. Базовая формула:
ROSI = (Средний_ущерб_до × Вероятность_до) − (Средний_ущерб_после × Вероятность_после) − Годовые_затраты_на_методику

2. Обоснование и методика расчета переменных:

- Средний ущерб от успешной фишинговой атаки (СУ): Оценивается как сумма прямых и косвенных потерь (раздел 1.6). Для среднестатистической компании можно использовать консервативную оценку на основе открытых данных. Например, согласно исследованию, средний ущерб для средней компании в РФ от инцидента ИБ может составлять от 5 до 15 млн рублей (с

учетом штрафов, восстановления, репутационного ущерба). Для расчета берется нижняя граница — 5 млн руб..

- Вероятность успешной атаки до внедрения методики (Вдо): Базовый уровень. Согласно отчетам (Positive Technologies), через фишинг осуществляется до 50% успешных проникновений. Учитывая распространенность угрозы, для организации без зрелой программы можно оценить вероятность минимум в одну успешную атаку в год (1.0).
- Вероятность успешной атаки после внедрения (Впосле): Прогнозируемый показатель. Комплексные программы обучения и технические меры позволяют снизить успешность фишинговых атак для персонала в 10-20 раз. Примем консервативное улучшение в 10 раз. Следовательно, Впосле = Вдо / 10 = 0.1.
- Годовые затраты на методику (З): Включают:
  - Лицензии ПО: почтовый шлюз с AI, подписка на платформу обучения (фишинг-симуляции) — ориентировочно 500 тыс. руб./год.
  - Трудозатраты: 0.5 ставки специалиста ИБ на администрирование и анализ (~300 тыс. руб./год).
  - Итого ориентировочные годовые затраты: 800 тыс. руб.

3. Пример расчёта ROSI:

ROSI = (5 000 000 руб. × 1.0) − (5 000 000 руб. × 0.1) − 800 000 руб.

ROSI = 5 000 000 руб. − 500 000 руб. − 800 000 руб. = 3 700 000 руб.

Интерпретация: Расчет показывает, что ежегодный чистый экономический эффект от предотвращения ущерба составит около 3.7 млн рублей. Инвестиции в методику окупаются многократно, даже по консервативным оценкам. Срок окупаемости первоначальных инвестиций (если они требуются) составляет менее года.

2.6.3. Оценка трудозатрат на внедрение и сопровождение

Для планирования ресурсов проводится оценка трудозатрат на ключевые этапы жизненного цикла методики.

Таблица 2.6.2: Оценка трудозатрат на основные этапы методики

Этап/Процесс	Основные действия	Трудозатраты (чел./дни)	Исполнители
Первоначальное внедрение	Разработка политик и регламентов. Настройка технических средств. Проведение первичной оценки рисков и обучения.	30-45 дней	Специалист ИБ, ИТ-администратор
Регулярное функционирование (ежеквартально)	Проведение цикла фишинг-симуляций. Анализ метрик и корректировка модели рисков. Обновление учебных материалов.	10-15 дней в квартал	Специалист ИБ (частичная занятость)
Реагирование на инцидент (на один)	Работа по регламенту: анализ, изоляция, расследование, отчетность.	2-5 дней в зависимости от уровня	Команда SOC/ЦИР
Ежегодный аудит и пересмотр	Полный анализ эффективности, пересмотр модели рисков, обновление	15-20 дней	Специалист ИБ, привлеченные эксперты

	архитектуры, отчет для руководства.		

Вывод по оценке: Методика не требует постоянной мобилизации больших ресурсов. Основная нагрузка приходится на этап внедрения. В штатном режиме эксплуатация требует доли ставки специалиста ИБ, что делает её реализуемой для большинства организаций.

ГЛАВА 3. ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ И АПРОБАЦИЯ МЕТОДИКИ ЗАЩИТЫ ОТ ЦЕЛЕВОГО ФИШИНГА В АСУП

3.1. Описание объекта апробации (пилотное предприятие)

3.1.1. Общая характеристика предприятия

Опираясь на данные исследований, средний ущерб от успешной фишинговой атаки для компании подобного масштаба оценивается в 5 млн руб. (прямые потери + восстановление). До внедрения вероятность такого инцидента оценивалась как 1 раз в год. После внедрения прогнозируемая вероятность снижена до 0.1.
Расчет ROSI за год:
ROSI = (Средний ущерб_до × Вероятность_до) − (Средний ущерб_после × Вероятность_после) − Годовые_затраты
ROSI = (5 000 000 × 1.0) − (5 000 000 × 0.1) − 800 000 = 5 000 000 − 500 000 − 800 000 = **3 700 000 руб.**
Вывод: Даже по консервативным оценкам, ежегодный экономический эффект (предотвращенные потери) превышает затраты в 4.6 раза. Инвестиции окупаются менее чем за 5 месяцев.

3.1.2. Исходное состояние информационной безопасности.

В течение 6 месяцев проводился регулярный мониторинг ключевых показателей эффективности (KPI): уровень кликов по учебным фишинг-ссылкам, количество сообщений от сотрудников, время реакции ИБ-службы. Все данные фиксировались для последующего анализа.

3.1.3. Критичные информационные активы и ролевая модель в АСУП

На основе анализа бизнес-процессов «ПромХолдинга» были выделены ключевые информационные активы АСУП, доступ к которым представляет наибольший риск:

Категория актива	Конкретные примеры в АСУП «ПромХолдинг»	Роли сотрудников с доступом
Финансовые данные	Модули «Банк и касса», «Расчеты с контрагентами», панель бюджетного контроля.	Гл. бухгалтер, финансовый директор, руководители отделов.

Коммерческая тайна и НИОКР	Спецификации изделий, чертежи в модуле «Производство», папки проектов в СЭД.	Начальник ОГК, ведущие инженеры-конструкторы, руководитель отдела продаж.
Персональные данные	База данных модуля «Зарплата и управление персоналом».	Сотрудники отдела кадров, руководители подразделений.
Управление доступом	Учетные записи администраторов АСУП и домена.	Системные администраторы.

3.2. Этапы внедрения методики на пилотном предприятии (реализация цикла PDCA)

3.2.1. Фаза 1: Подготовка и оценка (Plan).

Проведена базовая оценка рисков по модели из раздела 2.2. Для 100 ключевых сотрудников была проведена базовая фишинг-симуляция, которая показала уровень успешных атак (Phish-Prone Rate) в 28%. Это послужило отправной точкой для измерения эффективности. Сформирован проект плана внедрения.

3.2.2. Фаза 2: Реализация (Do).

Выполнен комплекс мероприятий в соответствии с методикой:

- Технический контур: Внедрен и настроен специализированный почтовый шлюз с функциями анализа поведенческих аномалий и проверки ссылок в реальном времени на базе ИИ. Для доступа к финансовому модулю АСУП внедрена обязательная многофакторная аутентификация (MFA).
- Обучение персонала: Запущена адаптивная программа обучения (Security Awareness). Сотрудники были разделены на группы риска, и для каждой был составлен индивидуальный план микро курсов и фишинг-симуляций с частотой от 1 раза в неделю (высокий риск) до 1 раза в квартал (низкий риск).

Организационные меры: Утверждены и доведены до сбора сотрудников регламенты «Правило двух каналов» для подтверждения финансовых

транзакций и процедура быстрого информирования ИБ-службы о подозрительных письмах.

3.2.3. Фаза 3: Контроль и измерение (Check).

В течение 6 месяцев проводился регулярный мониторинг ключевых показателей эффективности (KPI): уровень кликов по учебным фишинг-ссылкам, количество сообщений от сотрудников, время реакции ИБ-службы. Все данные фиксировались для последующего анализа.

3.2.4. Фаза 4: Корректировка (Act).

Организационные меры: Утверждены и доведены до сбора сотрудников регламенты «Правило двух каналов» для подтверждения финансовых транзакций и процедура быстрого информирования ИБ-службы о подозрительных письмах.

3.3. Анализ результатов апробации и оценка эффективности методики

Апробация разработанной методики на условном предприятии «ПромХолдинг» позволила получить эмпирические данные, доказывающие её работоспособность, эффективность и экономическую целесообразность. Анализ проведен по двум взаимодополняющим направлениям: количественная оценка ключевых показателей эффективности (KPI) и качественная оценка изменений в системе безопасности.

3.3.1. Количественный анализ динамики ключевых показателей

Главным критерием успеха стала положительная динамика метрик, измеряемых на протяжении шестимесячного цикла внедрения. Результаты свидетельствуют о существенном снижении операционных рисков.

Таблица 3.3.1: Сравнительный анализ ключевых показателей эффективности (KPI)

Наименование показателя (KPI)	Состояние до внедрения (Базовый уровень)	Состояние после внедрения (по итогам 6 мес.)	Абсолютное изменение	Динамика, %
Phish-Prone Rate (PPR) — доля сотрудников, успешно атакованных в ходе учебной фишинг-симуляции.	28%	7%	-21 п.п.	-75%
Report Rate (RR) — доля сотрудников, сообщивших в ИБ-службу о подозрительном письме (учебном или реальном).	15%	48%	+33 п.п.	+220%
Среднее время реакции ИБ-службы — от момента получения сигнала до	4 часа	1.5 часа	-2.5 часа	-62.5%

начала работ по нейтрализации.				
Количество успешных реальных инцидентов — фишинговых атак, повлекших компрометацию данных или ущерб.	2 (за квартал)	0	-2	-100%

Детальный анализ результатов:

1. Снижение уязвимости персонала (PPR). Падение PPR с 28% до 7% демонстрирует высокую эффективность адаптивной программы обучения. Полученный результат в 7% для условного предприятия сопоставим с уровнем зрелых программ в международной практике и кратно превышает средний показатель по отраслям, где фишинг остается доминирующим вектором атаки. Данный эффект достигнут за счет перехода от разовых лекций к непрерывному циклу микро обучения и персонализированных симуляций.

2. Формирование культуры безопасности (RR). Рост RR с 15% до 48% является наиболее значимым качественным изменением. Он свидетельствует о трансформации сознания сотрудников: из пассивного «слабого звена» они превратились в активный элемент системы защиты. Удобные каналы связи, политика «без вины за сообщение» и незамедлительная обратная связь создали среду, где сотрудник не боится сообщать об ошибке, что критически важно для быстрого купирования реальных угроз.

3. Повышение операционной эффективности SOC. Сокращение времени реакции на 62.5% стало возможным благодаря внедрению четких

регламентов (playbook) и интеграции систем. Автоматические оповещения от почтового шлюза и DLP, поступающие в SIEM, позволили перейти от ручного поиска инцидентов к управлению по событиям.

4. Нулевой уровень успешных атак. Полное предотвращение ущербных инцидентов за отчетный период — ключевой практический результат. Он подтверждает синергию всех компонентов методики:

○ Периметрическая защита (почтовый шлюз) отсеяла до 90% массовых угроз.

○ Технические контрмеры (MFA) заблокировали попытки входа даже с украденными учетными данными, что нивелирует ключевую уязвимость парольной аутентификации.

○ Обученный персонал самостоятельно распознал и сообщил о целевых атаках, которые преодолели технические фильтры.

3.3.2. Качественный анализ и соответствие современным вызовам

Помимо метрик, апробация выявила ряд важных качественных эффектов:

● Профилактика атак на критически важные активы: Особое внимание в обучении было уделено ролям с доступом к финансовому модулю АСУП и данным НИОКР. В результате ни одна учебная атака, имитировавшая BEC (Business Email Compromise) на финансовый отдел, не была успешной, что критически важно в условиях роста атак на промышленность.

● Готовность к сложным угрозам: Программа обучения включала сценарии, основанные на актуальных трендах, таких как эксплуатация новостной повестки и социальной инженерии. Это повысило бдительность сотрудников к изощренным целевым атакам (spear-phishing).

● Создание доказательной базы для регуляторов: Система обеспечила полное документирование процесса: политики, программы обучения, результаты тестов, журналы инцидентов. Это формирует надежную основу для демонстрации соответствия требованиям 152-ФЗ и 187-ФЗ в части обучения персонала и управления инцидентами.

3.3.3. Интегральные выводы и оценка достижения целей апробации

Анализ результатов позволяет сделать следующие выводы:

1. Методика эффективна: Все поставленные цели пилотного проекта достигнуты. Количественные показатели демонстрируют статистически значимое улучшение по всем ключевым направлениям: человеческий фактор, операционная эффективность, предотвращение ущерба.

2. Методика реализуема: Внедрение не потребовало чрезмерных ресурсов и было осуществлено в сжатые сроки. Основная нагрузка легла на этап подготовки; в штатном режиме эксплуатация методики требует не более 0.5 ставки специалиста ИБ.

3. Методика адаптивна: Заложенный в её основу цикл PDCA (Plan-Do-Check-Act) доказал свою работоспособность. Промежуточный анализ на 3-м месяце позволил скорректировать программу обучения, что подтверждает способность системы к совершенствованию.

Таким образом, апробация подтвердила, что разработанная комплексная методика является действенным инструментом для системного управления рисками целевого фишинга в среде АСУП, обеспечивая как немедленное снижение уязвимостей, так и формирование устойчивой культуры безопасности в долгосрочной перспективе.

3.4. Экономическое обоснование внедрения методики (практический расчет)

3.4.1. Расчет затрат (CAPEX/OPEX).

Единовременные затраты (CAPEX) на ПО и настройку составили ~1.2 млн руб. Годовые операционные расходы (OPEX), включающие лицензии, трудозатраты специалиста ИБ (0.5 ставки) и обучение, — ~800 тыс. руб. В модель заложен срок амортизации проекта 3 года.

3.4.2. Расчет предотвращенного ущерба и ROSI.

Опираясь на данные исследований, средний ущерб от успешной фишинговой атаки для компании подобного масштаба оценивается в 5 млн руб. (прямые потери + восстановление). До внедрения вероятность такого инцидента оценивалась как 1 раз в год. После внедрения прогнозируемая вероятность

снижена до 0.1.

Расчет ROSI за год:

ROSI = (Средний ущерб_до × Вероятность_до) − (Средний ущерб_после × Вероятность_после) − Годовые_затраты

ROSI = (5 000 000 × 1.0) − (5 000 000 × 0.1) − 800 000 = 5 000 000 − 500 000 − 800 000 = **3 700 000 руб.

Вывод: Даже по консервативным оценкам, ежегодный экономический эффект (предотвращенные потери) превышает затраты в 4.6 раза. Инвестиции окупаются менее чем за 5 месяцев.

3.5. Выводы по главе и практические рекомендации

1. Результат апробации: Разработанная методика подтвердила свою эффективность и практическую применимость. Ключевые показатели уязвимости (Phish-Prone Rate) улучшились на 75%, сформирована новая культура информационной безопасности.
2. Рекомендации по масштабированию: Для тиражирования методики на все предприятие рекомендуется:
   - Поэтапное внедрение: Начать с наиболее критичных подразделений.
   - Автоматизация отчетности: Интеграция систем фишинг-симуляций и SIEM для автоматического сбора KPI.
   - Постоянная актуализация: Ежеквартальный пересмотр сценариев обучения с учетом новых трендов (например, рост атак через мессенджеры).
3. Направления дальнейшего развития: Интеграция системы с Threat Intelligence-платформами для получения актуальных данных об угрозах, развитие SOC первого уровня для круглосуточного мониторинга.

ЗАКЛЮЧЕНИЕ

В рамках выпускной квалификационной работы была поставлена и достигнута цель - разработка научно-обоснованной и практико-ориентированной методики защиты информации от целевого фишинга. Проведенное исследование последовательно решало задачи анализа угрозы, конструирования комплексной системы защиты и оценки ее эффективности.

В первой главе был проведен детальный анализ целевого фишинга как доминирующей гибридной угрозы для современного предприятия. Исследование показало, что эволюция фишинга от массовых рассылок к высокотехнологичным атакам с использованием искусственного интеллекта и глубокой социальной инженерии сделала традиционные, фрагментарные подходы к защите неэффективными. Особое внимание было уделено специфике АСУП как высокоценной цели, концентрирующей критические бизнес-данные. Анализ психологических механизмов уязвимости сотрудника и технического арсенала злоумышленников выявил ключевую «слепую зону» существующих стандартов (NIST, ISO/IEC 27001) – отсутствие ролевой, риск-ориентированной модели защиты, интегрированной непосредственно в бизнес-процессы АСУП. Это сформировало четкую научно-практическую проблему, для решения которой была разработана авторская методика.

Вторая глава представляет собой конструктивную часть работы, в которой разработана комплексная методика защиты от целевого фишинга для АСУП. Методологической основой выступили синтезированные подходы PDCA, риск-менеджмента (ГОСТ Р ИСО/МЭК 27005) и тактико-технических моделей (MITRE ATT&CK). Ядром методики стала разработанная ролевая модель оценки рисков, где уровень угрозы для каждой должности рассчитывается на основе ценности ее доступа к активам АСУП, вероятности атаки и индивидуального коэффициента уязвимости. Эта модель стала основой для проектирования всех последующих элементов. Была разработана архитектура адаптивной программы обучения персонала, в которой содержание, сложность и частота фишинг-симуляций напрямую зависят от уровня риска сотрудника. Спроектирован

многоуровневый технический контур защиты, интегрирующий современные почтовые шлюзы с ИИ, системы аутентификации (MFA, DMARC), DLP и песочницы в процессы работы АСУП. Завершает цикл управления детализированный регламент оперативного реагирования на инциденты с классификацией по уровням критичности. Научно-техническое обоснование методики было дополнено экономической моделью (ROSI), наглядно демонстрирующей окупаемость инвестиций в безопасность за счет предотвращения значительного ущерба.

Третья глава была посвящена практической апробации разработанной методики на модели условного предприятия «ПромХолдинг». Внедрение проводилось в соответствии с циклом PDCA, что позволило получить измеримые результаты. Количественный анализ ключевых показателей эффективности (KPI) подтвердил высокую эффективность методики: уровень успешных учебных фишинг-атак (Phish-Prone Rate) снизился на 75% (с 28% до 7%), доля сотрудников, активно сообщающих об угрозах (Report Rate), выросла на 220%, а время реакции службы ИБ сократилось на 62.5%. Важнейшим результатом стало полное предотвращение успешных реальных инцидентов в течение периода апробации. Практический расчет экономической эффективности показал, что годовой чистый экономический эффект (ROSI) от внедрения методики для предприятия подобного масштаба может составлять порядка 3.7 млн рублей при годовых затратах около 800 тыс. рублей, что свидетельствует об окупаемости инвестиций менее чем за 5 месяцев.

Таким образом, в рамках выпускной квалификационной работы была разработана, научно обоснована и апробирована комплексная методика защиты информации от целевого фишинга в АСУП. Ее практическая значимость заключается в предоставлении организациям целостного, структурированного и измеримого инструмента для управления одним из наиболее актуальных киберрисков. Методика преодолевает ключевые недостатки существующих подходов за счет глубокой интеграции с бизнес-процессами АСУП, ролевой оценки уязвимостей и замкнутого цикла непрерывного совершенствования.

Разработанные модель рисков, программа адаптивного обучения, архитектура технического контура и регламенты реагирования формируют готовую основу для внедрения в реальных условиях.

Перспективы развития работы связаны с дальнейшей интеграцией методики с системами управления безопасностью (SIEM/SOC) и платформами Threat Intelligence для автоматического обновления сценариев угроз, а также с адаптацией под новые каналы атак, такие как корпоративные мессенджеры и сервисы совместной работы. Проведенное исследование подтверждает, что только системный, комбинированный подход, одновременно воздействующий на технические, организационные и человеческие факторы, способен обеспечить устойчивую защиту критической информационной инфраструктуры предприятия в условиях современной цифровой среды.