Фишинг: анализ цифровой угрозы и гид по медиабезопасности

Итоговый проект по дисциплине «Цифровые технологии и медиабезопасность»

Автор: Заварзин А.В., группа ИИ/б-25-6-о

Курс: Специализированная мастерская «Цифровой офис. Промт-инжиниринг для повседневных задач»

Что такое фишинг и почему это актуально?

Фишинг — это вид интернет-мошенничества, цель которого — кража конфиденциальных данных (логины, пароли, данные карт) через поддельные письма и сайты, маскирующиеся под легитимные организации (банки, службы доставки).

Ключевые признаки фишингового сообщения:

- Давление и срочность в сообщении.
- Подозрительные ссылки и адреса отправителей.
- Орфографические ошибки и нетипичные приветствия.
- Незапрашиваемые вложения.

> **Актуальность:** По данным «Лаборатории Касперского», фишинг является причиной более 90% всех утечек данных. Это ежедневная реальность, а не просто «страшилка».

Примеры реальных фишинговых атак

Киберпреступники постоянно совершенствуют свои методы, адаптируясь под новые реалии и технологии. Эти кейсы демонстрируют разнообразие и изощренность фишинговых атак.

Кейс 1: Целевой фишинг криптокошельков

Атаки через Google Forms, маскирующиеся под сервисы поддержки криптокошельков, с целью запроса сид-фразы для доступа к активам жертвы. **Уязвимость:** Доверие к знакомым платформам.

Кейс 2: Массовая рассы л ка от Microsoft

Поддельные уведомления о «неудачных попытках входа» в аккаунт Microsoft, призывающие немедленно сменить пароль по фишинговой ссылке. **Уязвимость:** Страх потери доступа и спешка.

Кейс 3: «Китобойный» фишинг (Whaling)

Целевые атаки на высокопоставленных сотрудников через LinkedIn, имитирующие письма от руководства с требованием «срочных переводов». **Уязвимость:** Иерархия и исполнение приказов.

Для кого создается гид? Уязвимости разных групп

Эффективная защита требует понимания специфических рисков каждой группы пользователей. Наш гид разработан с учётом этих особенностей.

Школьники (7 класс)

Наиболее уязвимы к фишингу в социальных сетях и мессенджерах, часто через ссылки «от друзей», предложения об участии в розыгрышах или онлайн-играх. Их неопытность и желание получить что-то бесплатно делают их легкой мишенью.

Пожилые люди

Часто становятся жертвами мошенничества, имитирующего звонки от банков, государственных органов или медицинских учреждений. Незнание цифровых технологий и чрезмерное доверие к авторитетам — их главные уязвимости.

Научные сотрудники

Подвержены целевому фишингу, направленному на компрометацию корпоративных данных, доступ к научным сервисам или интеллектуальной собственности. Их профессиональная деятельность требует доступа к чувствительной информации, что делает их привлекательной целью.

Адаптированные алгоритмы защиты для каждой аудитории

Разработанные рекомендации учитывают особенности каждой целевой группы, предоставляя практические и легко применимые советы для повышения медиабезопасности.

Не кликай сразу! Всегда проверяй источник и контекст сообщения, прежде чем переходить по ссылке.	**Не спеши переводить деньги!** Мошенники часто создают ощущение срочности.	**Верифицируй email отправителя до символа!** Даже одно отличие может указывать на фишинг.
Спроси у друга голосом! Если пришло сообщение от друга с подозрительной ссылкой, лучше переспроси лично или по звонку.	**Позвони по известному номеру, чтобы проверить!** Никогда не перезванивай по номеру из подозрительного письма или сообщения.	**Используй двухфакторную аутентификацию (2FA)!** Это дополнительный уровень защиты, который значительно усложняет взлом аккаунта.
Зайди в аккаунт напрямую, а не по ссылке из письма! Всегда вводи адрес сайта вручную в браузере.	**Игнорируй угрозы по почте от «госорганов»!** Официальные структуры никогда не будут требовать данные или угрожать по электронной почте.	**Все подозрительные письма — в ИТ-отдел!** Сообщай о любых подозрительных сообщениях для оперативного анализа и предотвращения атак.

Визуальный язык гида: метафоры и дизайн

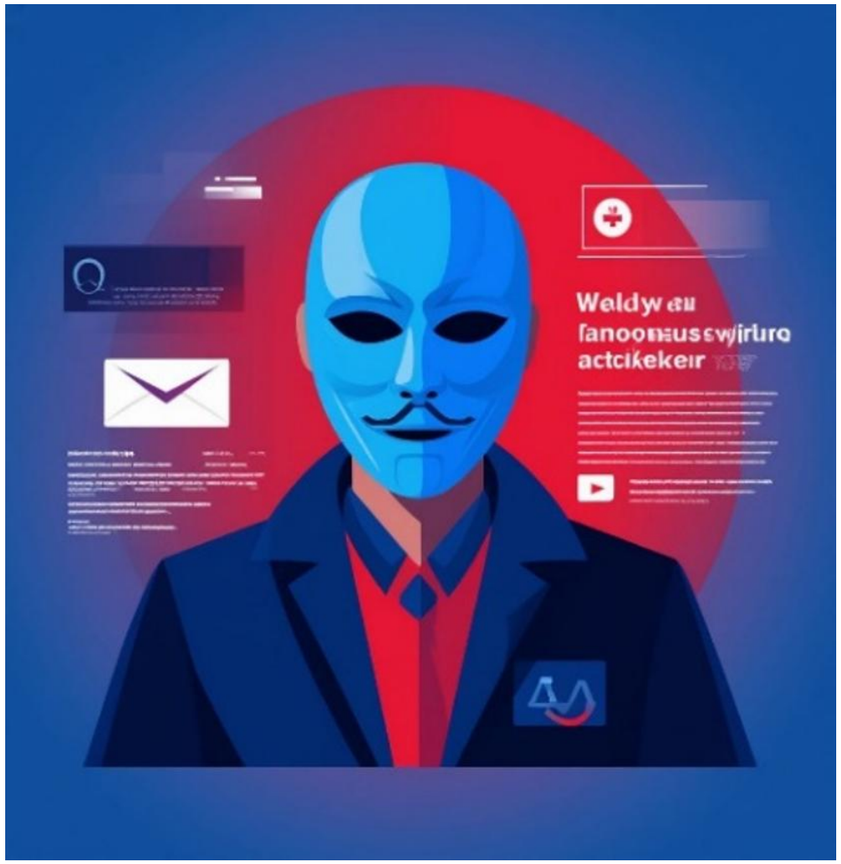
Эффективный гид должен быть не только информативным, но и привлекательным. Наш дизайн использует цветовую психологию и яркие метафоры для лучшего восприятия.

Цветовая палитра:

- Тёмно-синий (#2E5BFF): доверие, серьёзность, профессионализм.
- Красный (#FF4757): акцент опасности, предупреждение, угроза.
- Голубой (#26E8C8): технологичность, современность, чистота.
- Светло-серый (#F5F7FA): нейтральность, фон, сбалансированность.

Ключевые метафоры-иллюстрации:

- Рыболовный крючок в форме конверта: символ письма-приманки.
- Письмо с маской: анонимность и обман злоумышленника.
- Защитный щит, отражающий письма: активная защита от угроз.
- Увеличительное стекло, выявляющее поддельные элементы: внимательность и анализ.



Функциональная модель системы обнаружения фишинга (Use Case)

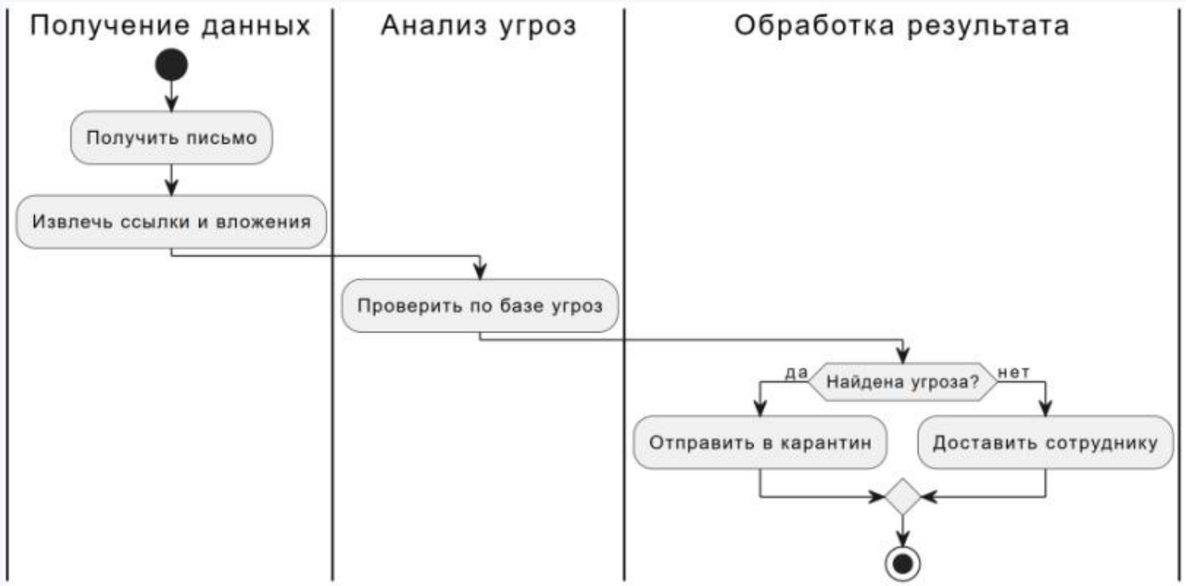
Разработанная модель описывает взаимодействие пользователей с системой, обеспечивая замкнутый цикл безопасности: обнаружение → анализ → реакция → улучшение правил.

Основные акторы системы:

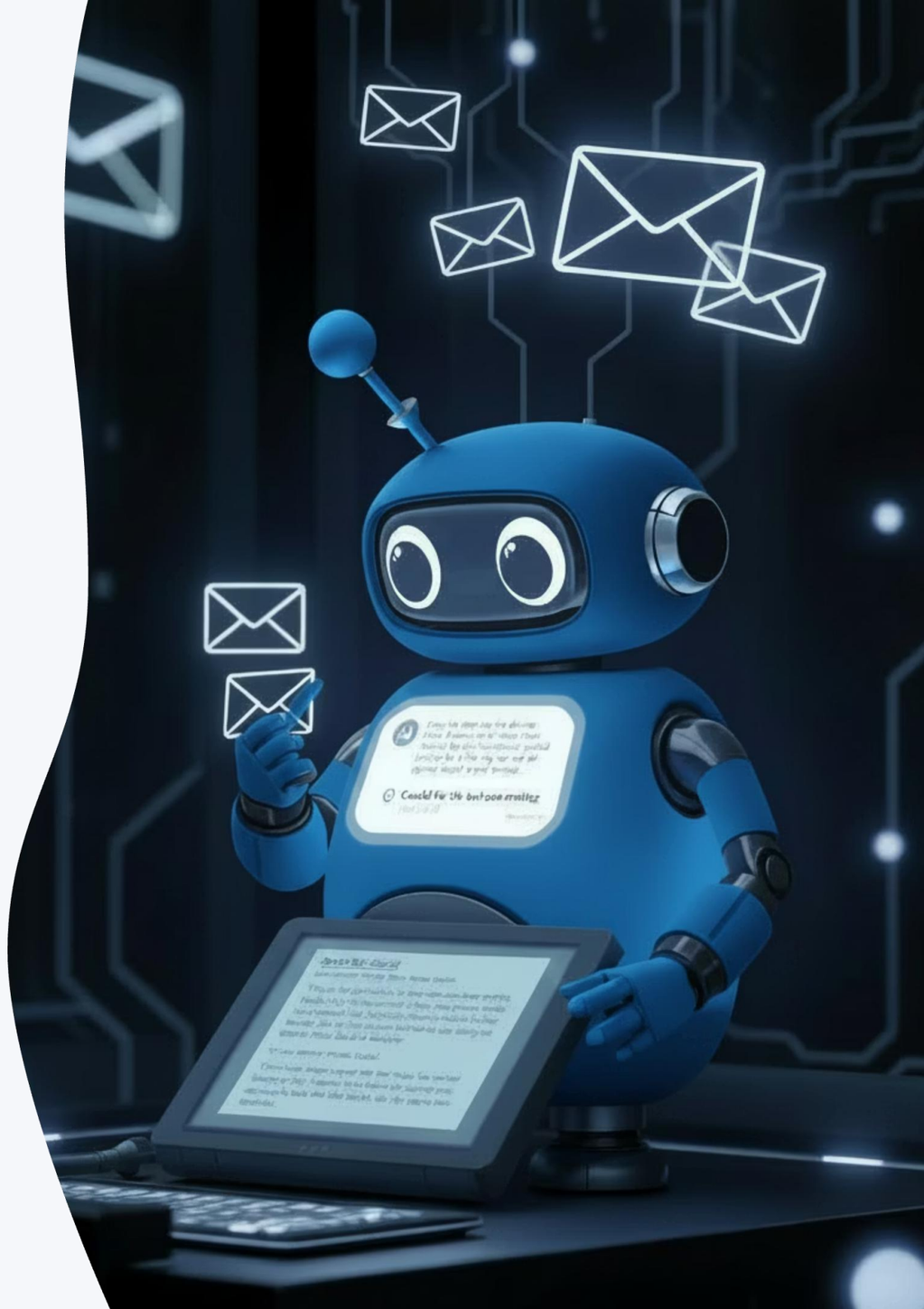
- **Сотрудник:** Получает письма, информирует о подозрительных сообщениях.
- **Администратор:** Управляет правилами фильтрации, мониторит отчёты.
- **Система анализа:** Автоматически проверяет письма, формирует аналитические данные.

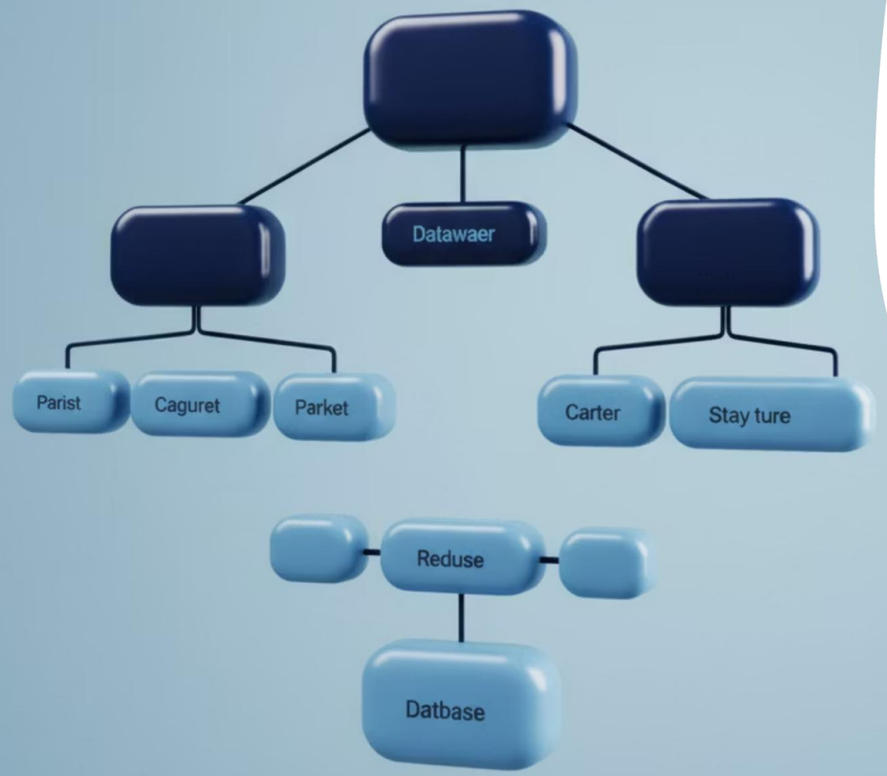
Алгоритм автоматического анализа входящего письма (Activity Diagram)

Представленная блок-схема иллюстрирует последовательность действий, которые выполняет система при получении каждого нового электронного письма, обеспечивая проактивную защиту.



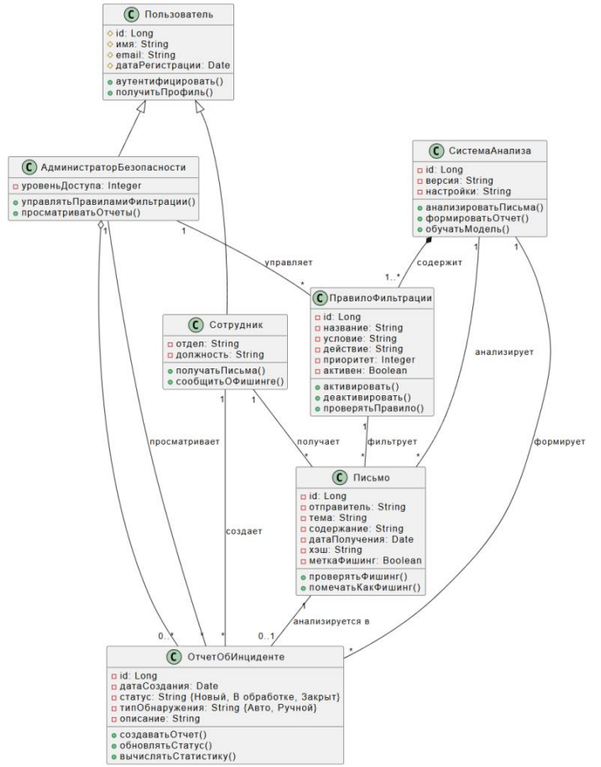
Этот алгоритм позволяет минимизировать риск попадания фишинговых писем в почтовые ящики пользователей, автоматизируя процесс их обнаружения и изоляции.





Ключевые сущности системы (Class Diagram)

Диаграмма классов описывает структуру данных и взаимосвязи между основными компонентами системы обнаружения фишинга, лежащие в основе её функциональности.



Основные классы и их атрибуты

- **Письмо:** Отправитель, Тема, Статус (доставлено, в карантине), Хэш-сумма, Метка «фишинг».
- **Отчёт об инциденте:** Идентификатор, Уровень угрозы, Статус (Новый, В обработке, Закрыт).
- **Правило фильтрации:** Условие (что искать), Действие (что делать), Приоритет.
- **Пользователь:** Родительский класс для **Сотрудника** и **Администратора**, определяющий общие характеристики.

Выводы и результаты проекта

Этот проект продемонстрировал комплексный подход к борьбе с фишингом, сочетая глубокий анализ угрозы, практические рекомендации и техническое проектирование.

Анализ угроз

Проведён глубокий анализ угрозы фишинга и классификация реальных кейсов атак.

Адаптированный гид

Разработан персонализированный гид по безопасности для различных групп пользователей.

UML-моделирование

Спроектирована функциональная модель системы обнаружения фишинга с помощью UML.

Промпт-инжиниринг

Получены и применены ключевые навыки промт-инжиниринга для работы с ИИ.

Финальный тезис: Комплексный подход от анализа до реализации инструментов — ключ к эффективной медиабезопасности в цифровом мире.