ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
Институт компьютерных технологий и информационной безопасности
Кафедра безопасности информационных технологий
Выпускная квалификационная работа

СИСТЕМА АНТИФИШИНГОВЫХ УЧЕНИЙ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

Научный руководитель ВКР, к.т.н., доцент кафедры БИТ Абрамов Е.С.
Исполнитель студент группы КТсо5-5 Гузиев М.М.


Personal
Data

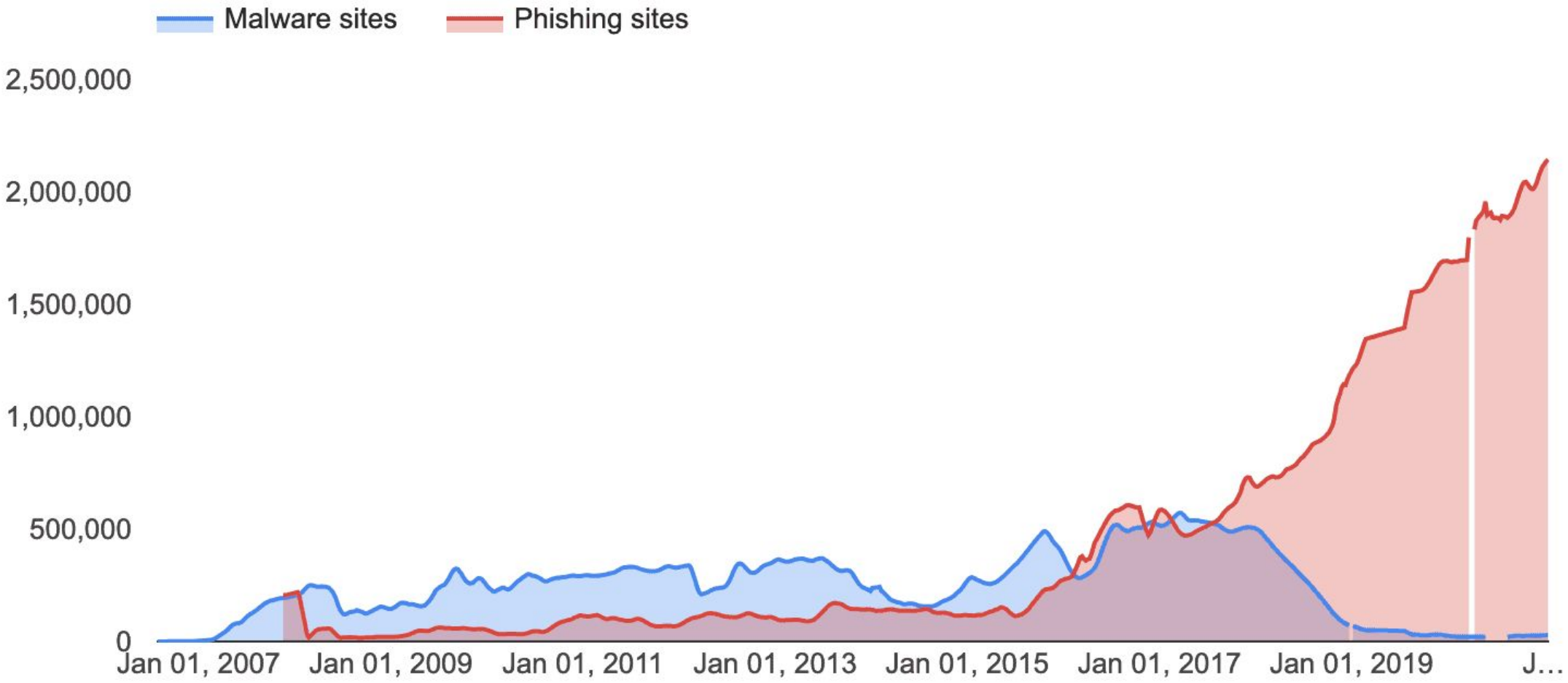
Цели исследования

1. Описать теоретические основы фишинга и антифишинга.
2. Проанализировать аналогичные решения по предотвращению фишинга и обучению пользователей.
3. Разработать концепцию проведения антифишинговых учений.
4. Разработать архитектуру системы антифишинговых учений.
5. Исследовать безопасность человеко-машинного взаимодействия.
6. Провести технико-экономическое обоснование.

Основные цели антифишинговых учений :

1. Обучить пользователей распознавать фишинговые атаки, сообщать о них и избегать их, что поможет защитить их и кафедру/отдел от киберугроз.
2. Помочь службе ИБ собирать более качественные показатели и информацию об атаках с использованием электронной почты, чтобы лучше защитить сеть от этих угроз.

Актуальность



Увеличение числа фишинговых сайтов 2007-2021

Основные типы фишинга

1. Фишинг по электронной почте.
    1. Массовая рассылка (десятки тысяч – миллионы сообщений)
    2. Письма нацелены на то, чтобы вызвать эмоцию и мгновенное действие.
2. Целевой фишинг.
    1. Нацелен на конкретного человека или предприятие.
    2. Злоумышленник хорошо осведомлён о внутренних процессах компании, именах и ролях сотрудников.

Сценарий фишинговой кампании

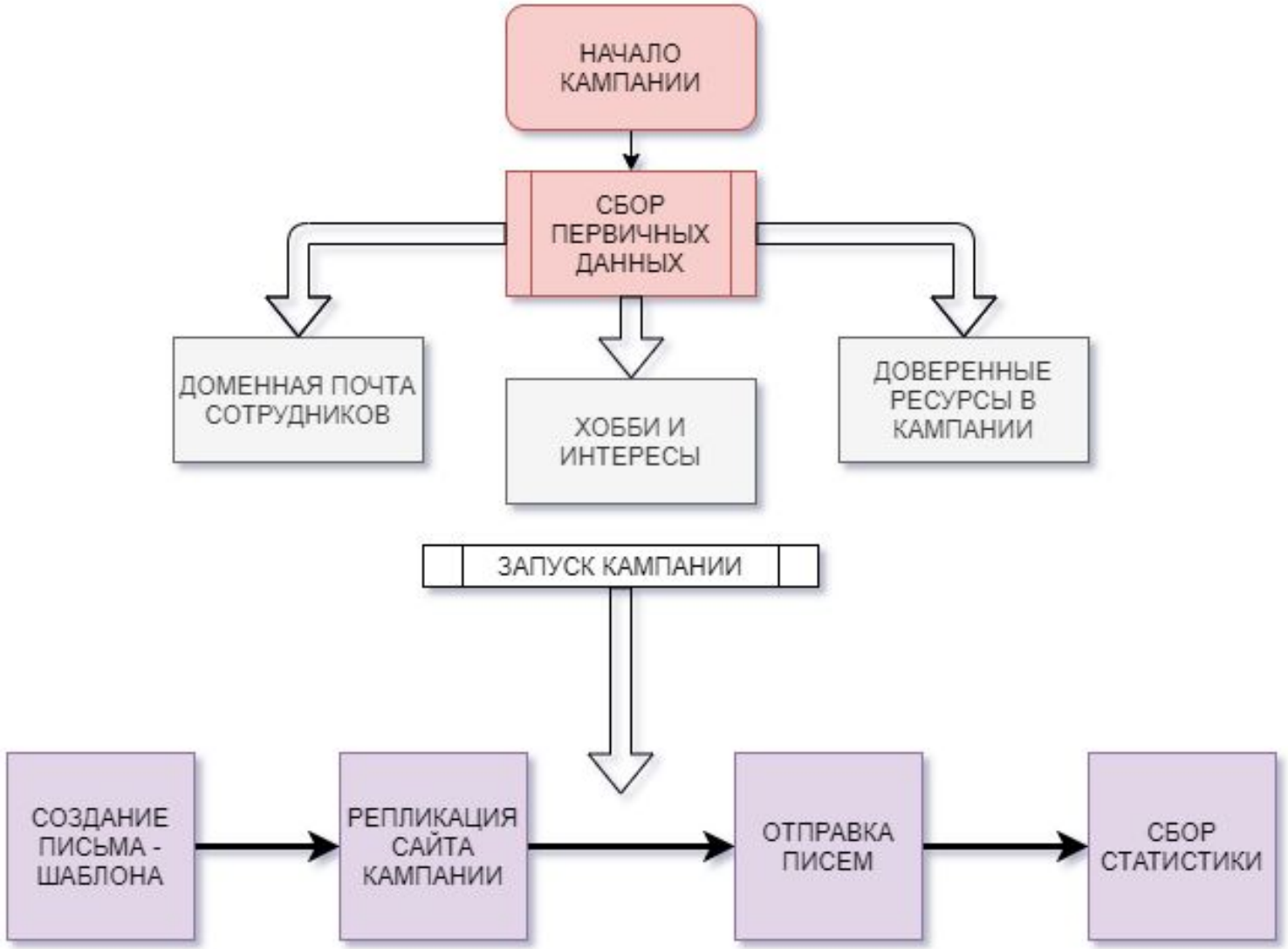


Схема фишинговой атаки на основе e-mail рассылки

Структура фишингового сообщения 1

Тема: Расчетный лист

Уважаемый сотрудник!

В соответствии со статьей 136 ТК РФ направляем в Ваш адрес расчетный лист.

Просмотр расчетного листа теперь доступен на портале SFEDU.RU.

По всем вопросам, касающимся заработной платы, просьба обращаться в часы приема:

Понедельник с 9.00 до 12.30

Вторник с 13.00 до 16.30

Среда нет приема

Четверг с 13.00 до 16.30

Пятница с 9.00 до 12.30

Кабинеты: 407, 409

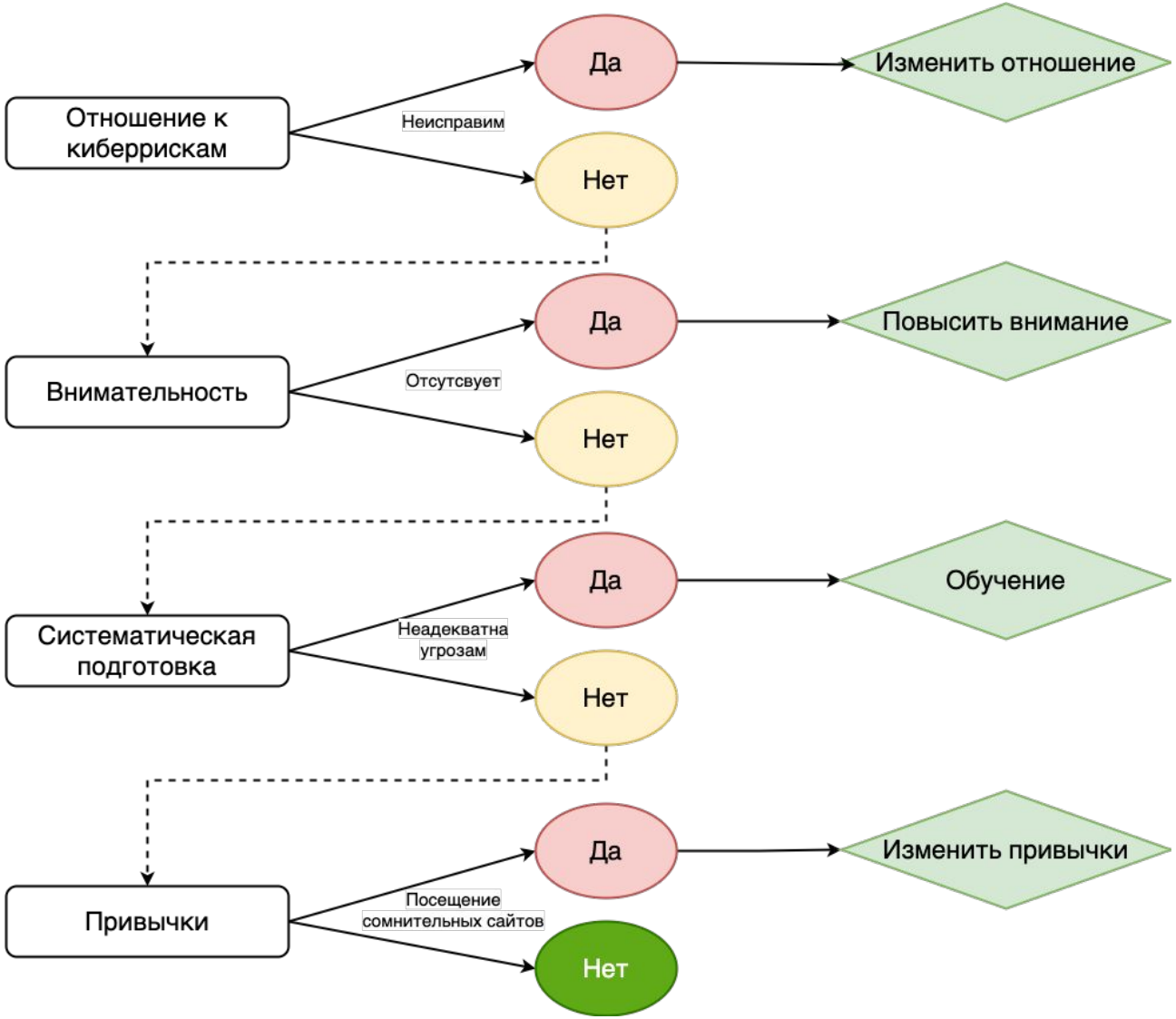
Телефоны: 218-40-72; 218-40-48; 218-40-76; 218-40-20

С уважением, заместитель главного бухгалтера ЮФУ

sfedu.ru.forour.info/1/index.php

Логотип для создания солидности и официальности

Алгоритм определения потенциальной жертвы фишинга

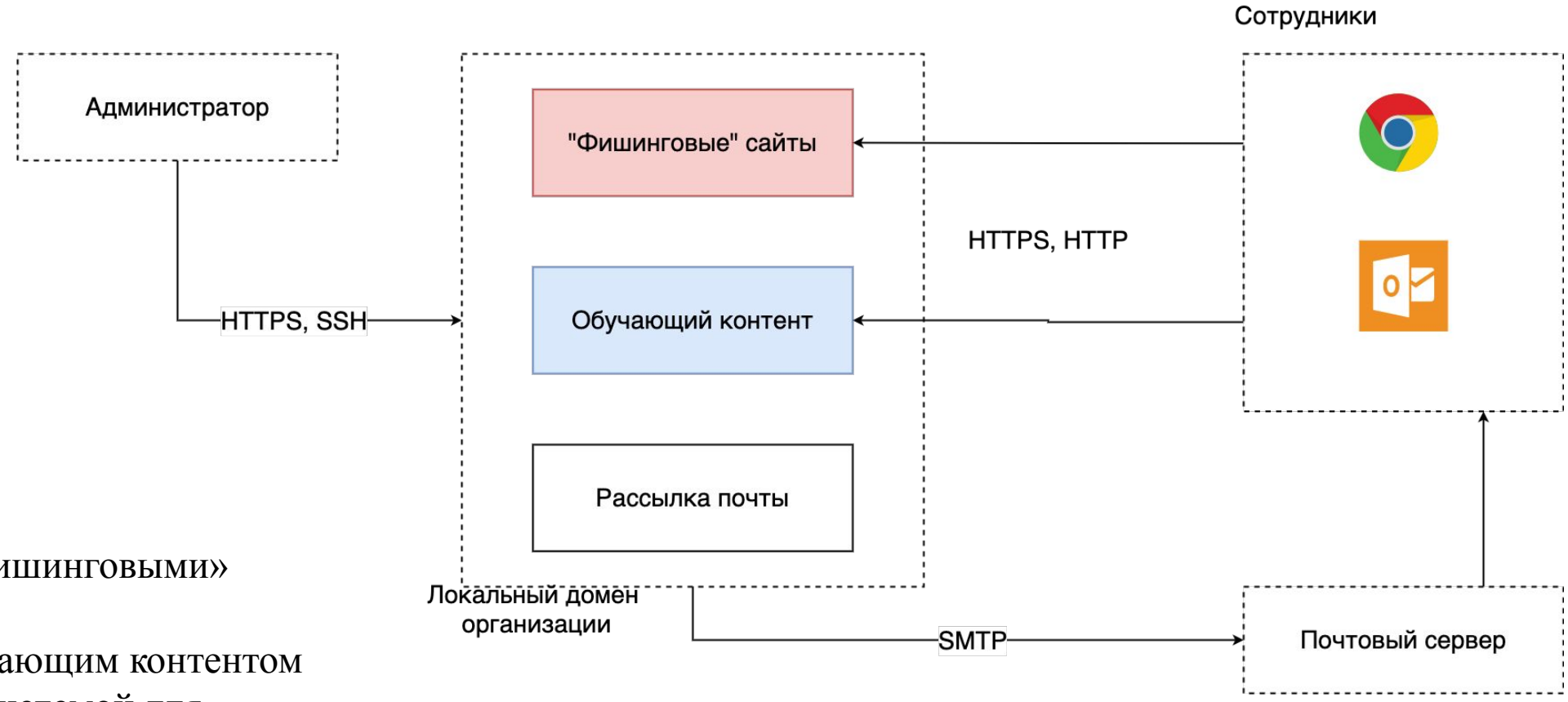


Создание опросника для выявления целей обучения

Темы обучения

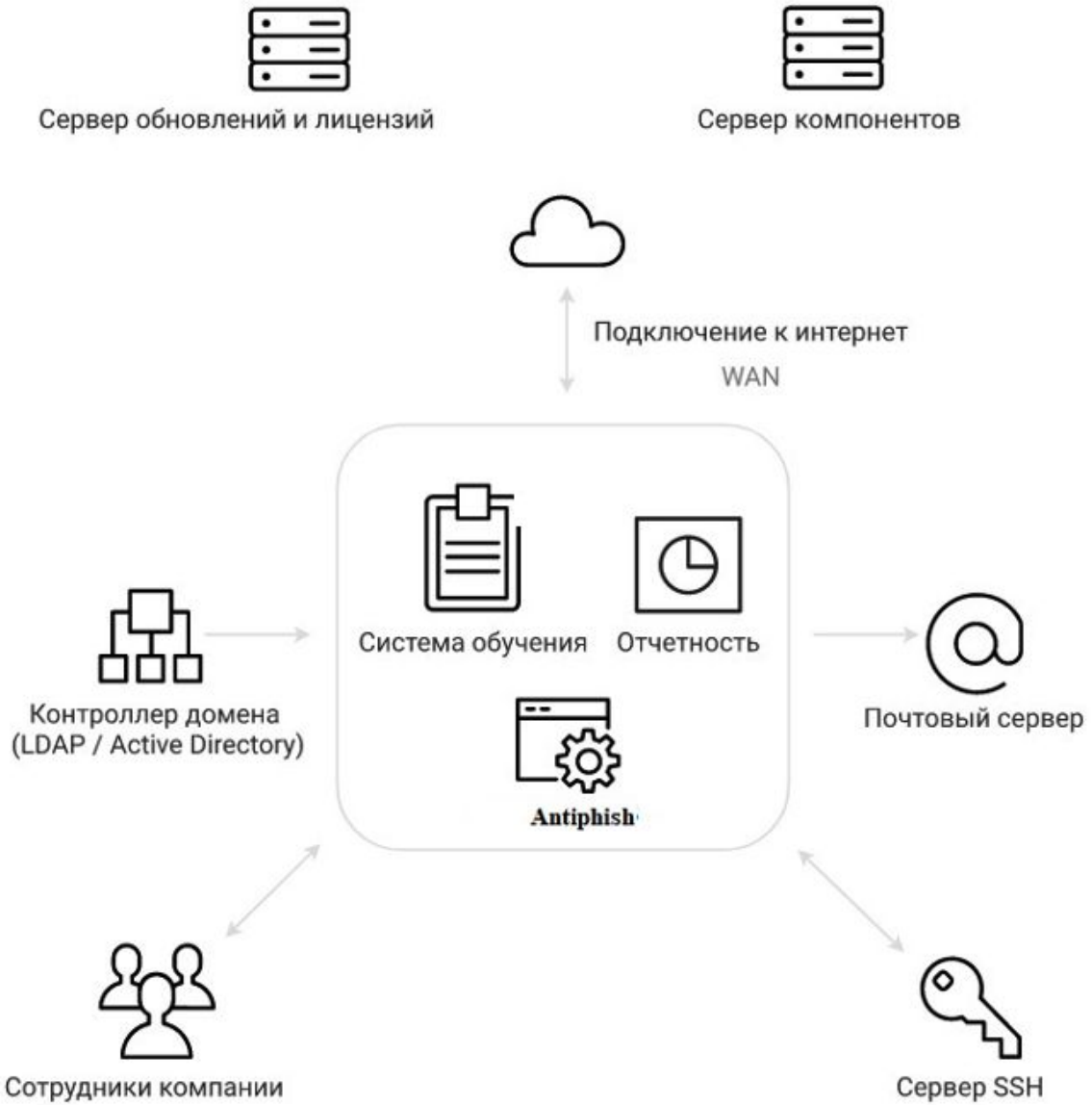
1. Текущие угрозы.
2. Признаки атаки.
3. Защитные процедуры.
4. Планы реагирования на угрозы.

Схема работы системы антифишинговых учений



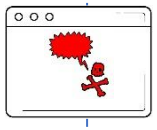
1. Контейнеры с «фишинговыми» сайтами.
2. Контейнер с обучающим контентом
3. Контейнер с подсистемой для рассылки «фишинговых» сообщений.

Архитектура системы



Сценарий работы системы антифишинговых учений

Для каждого работника подготавливается
письмо-ловушка под специфику его работы



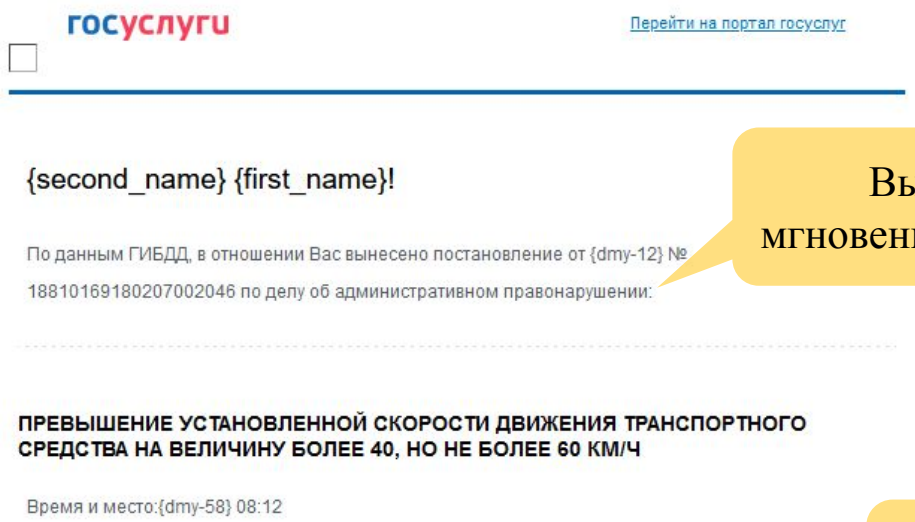
Работник открывает «вредоносные» файлы и ссылки в «письме-ловушке»

Ответственный работник видит пользователей открывших вложение
Формируется отчёт со списком лиц, нарушивших требования политики ИБ

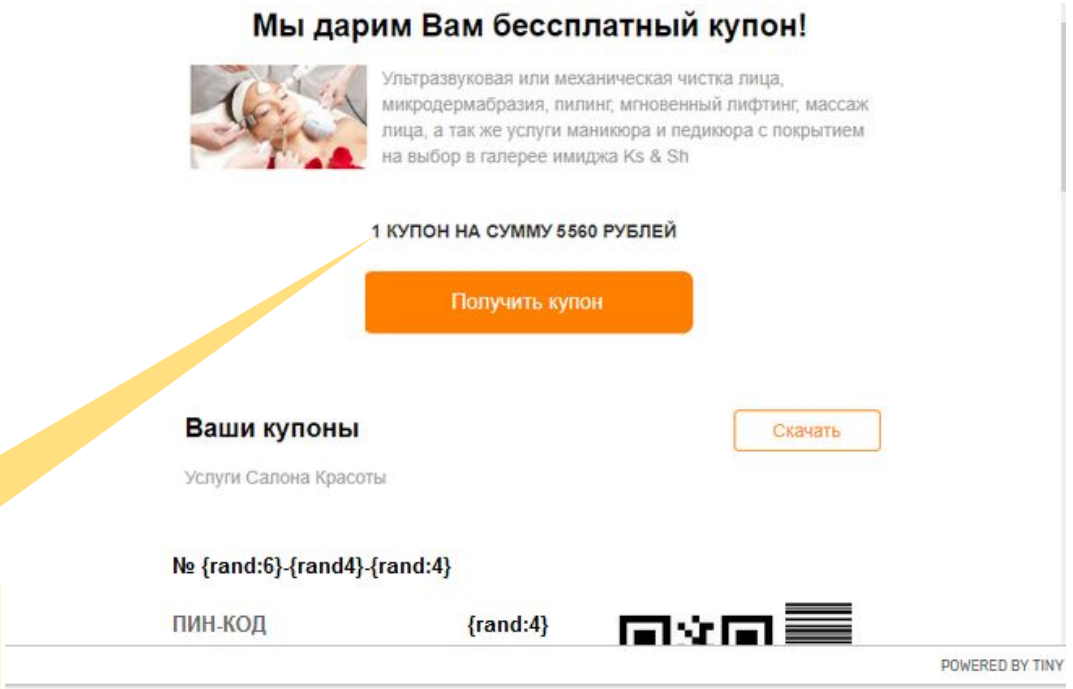
Проводится онлайн-обучение для работников, нарушивших требования политики ИБ

Проверка работников и их последующее обучение проходит на регулярной основе

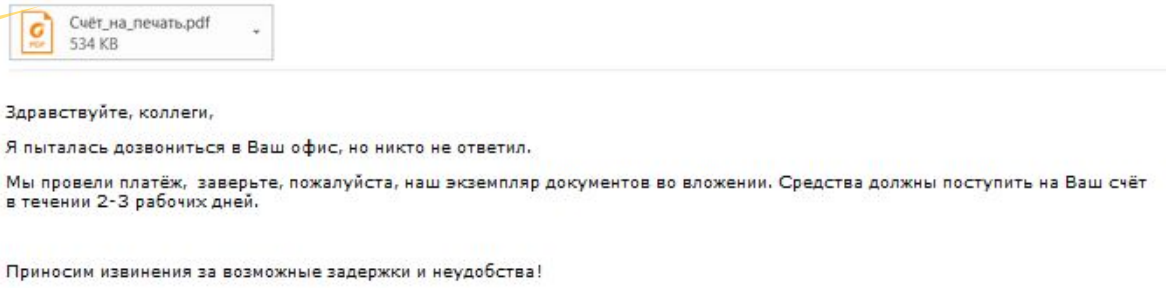
Некоторые популярные шаблоны «фишинговых» писем



Вызвать мгновенные эмоции



Халява!



Самый популярный тип - платёжки

В ВКР подробно рассмотрено 8 различных шаблонов

Меры противодействия фишингу

1. Будьте в курсе методов фишинга.
2. Не нажимайте на ссылки, не загружайте файлы и не открывайте вложения в электронных письмах от неизвестных отправителей.
3. Никогда не отправляйте по электронной почте личную или финансовую информацию, даже если вы близки с получателем.
4. Никогда не вводите личную информацию во всплывающем окне. Это никогда не бывает хорошей идеей.
5. Обновляйте свой браузер.
6. Установите антифишинговую панель инструментов.
7. Двухфакторная аутентификация (2FA) является наиболее эффективным методом противодействия фишинговым атакам, поскольку она добавляет дополнительный уровень проверки при входе в конфиденциальные приложения, и защищает при краже основного пароля.
8. Применять строгие политики управления паролями.
9. Образовательные кампании также могут помочь уменьшить угрозу фишинговых атак.

Заключение по безопасности человеко-машинного взаимодействия

Условия труда при разработке условно относят к безопасным. Поэтому для поддержания высокого уровня работоспособности и сохранения здоровья работника, необходимо соблюдать регламентированные требования СП 2.2.3670-20. Инженеру по безопасности нужно учитывать время регламентированного отдыха для предупреждения преждевременной утомляемости (устраивать перерывы на 10 - 15 мин. через каждые 45 - 60 мин. работы). Также целесообразно во время перерывов выполнять комплексы упражнений для предотвращения возникновения гиподинамии, а также упражнений от усталости глаз, для предотвращения сухого кератоконъюнктивита или синдрома «сухого глаза».

Заключение по технико-экономическому обоснованию

Стоимости разработки рассмотренных систем примерно сопоставимы. Достоинством аналога является его фактическое наличие и возможность пользоваться технической поддержкой при заключении официального контракта на использование. Недостатки:

- Высокая стоимость ежегодной лицензии.
- Высокий период окупаемости.
- Возможные ограничения лицензионной политики поставщика.
- Возможное внедрение вредоносных функций в код open-source проектов.

Разработка и последующее использование собственной системы имеет следующие преимущества:

- Низкая стоимость
- Высокая маржинальность коммерческих сервисов
- Полные права на платформу
- Отсутствие лицензионных ограничений
- Позволит после внедрения собственной платформы провести сравнительное тестирование с коммерческими продуктами.

Согласно полученным результатам, качество собственной разработки является более высоким, чем качество рассмотренного аналога. Коэффициент качества собственной разработки 1,38, следовательно, система по техническим параметрам превосходит аналог.

Выводы

1. Фишинг - это актуальная угроза.
2. Адреса электронной почты можно подделать.
3. Строки темы письма и текст стараются вызвать эмоциональный отклик пользователя.
4. Атаки становятся более целенаправленными.
5. Фишинговые электронные письма становятся все более качественно сделанными.
6. Ссылки не всегда то, чем кажутся.
7. Фишинговые ссылки можно скрыть во вложениях.
8. Хакеры используют настоящие изображения и логотипы брендов.
9. Обучение осведомленности о фишинге должно быть постоянным процессом.