ВУРАСКО АЛЕКСАНДР

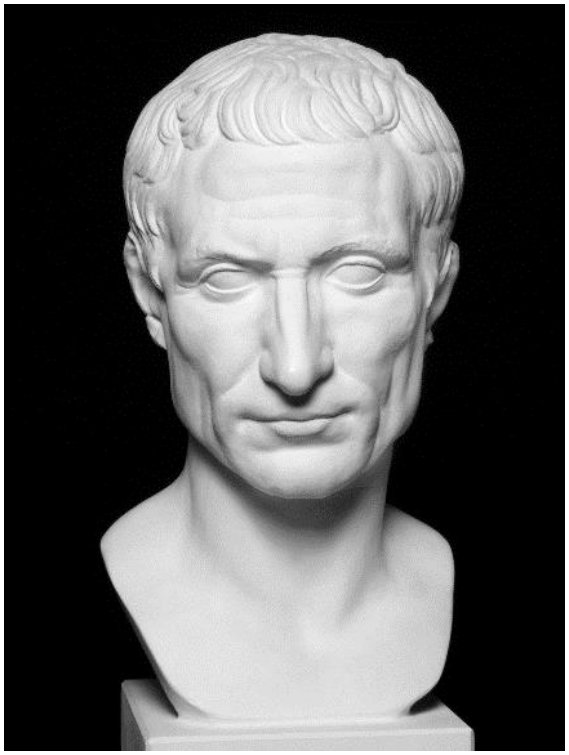
ведущий аналитик
Infosecurity
a Softline company

vurasko@in4security.com

Механизмы обеспечения ИБ:

- Организационные
- Технические

Римская империя, I век до нашей эры



Технические методы	Организационные методы
Использование «Шифра Цезаря» при передаче сообщений.	• Вооруженная охрана курьеров. • Хранение посланий в закрытых шкатулках. • Контроль доступа к корреспонденции

СТАТИСТИКА

~50%

веб-приложений
содержат уязвимости

~129 дней

уходит на исправление
критической уязвимости

56%

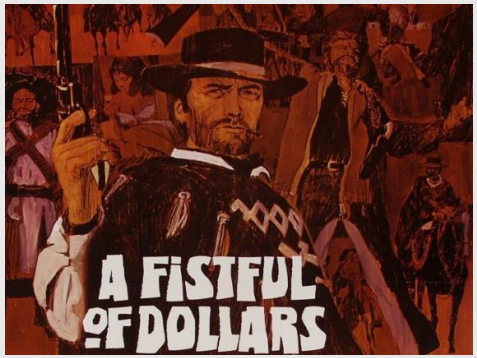
доля систем с тривиальной
сложностью преодоления
сетевого периметра

36%

доля успешных атак
с получением доступа
к конфиденциальным данным

** по данным Application Security Statistics Report 2017 и Positive Technologies за 2016-2018 гг.*

Популярность высоких технологий у современных преступников



Концепция: «киберпреступление как услуга»:
- низкий порог вхождения
- доступный инструментарий для совершения преступлений
- не нужно обладать глубокими познаниями в IT-сфере

Широкий круг охвата потенциальных жертв

Простота вывода денежных средств

Транснациональный характер сети

Возможности анонимизации

ЦЕЛИ И РЕЗУЛЬТАТЫ

Обнаружение уязвимостей и подготовка рекомендаций по их устранению

Определение направлений дальнейшего совершенствования системы ИБ

Устранение уязвимостей в инфраструктуре компании

Выполнение требований контролирующих органов и соблюдение стандартов

Обоснование бюджета на повышение уровня ИБ

СТАНДАРТЫ И МЕТОДОЛОГИИ

Приказы ФСТЭК России № 17, 21, 31

Международная программа
Certified Ethical Hacker

Standards for Information Systems Auditing
(ISACA)

OSSTMM v3.0 (Open Source Security Testing
Methodology Manual)

OWASP Testing Guide v4

СЦЕНАРИИ ТЕСТИРОВАНИЯ

BLACK BOX

Пентестер воспроизводит действия внешнего злоумышленника, имеющего общее представление об атакуемых объектах из открытых источников.

GREY BOX

Пентестер имитирует действия хакера, обладающего знаниями об атакуемом объекте. Уровень и глубина знаний определяется заказчиком.

WHITE BOX

Пентестер обладает всеми правами доступа администратора, и имеет полное представление об инфраструктуре организации.

ВИДЫ ПЕНТЕСТОВ

Внешний пентест и тестирование веб-приложений (Black, Grey box)

Внутренний пентест информационных систем (Black, Grey box)

Пентест точек доступа Wi-Fi (Black box)

Социотехнический пентест (Black, Grey box)

Внутренний аудит безопасности (White box)

Структура современного преступного сообщества

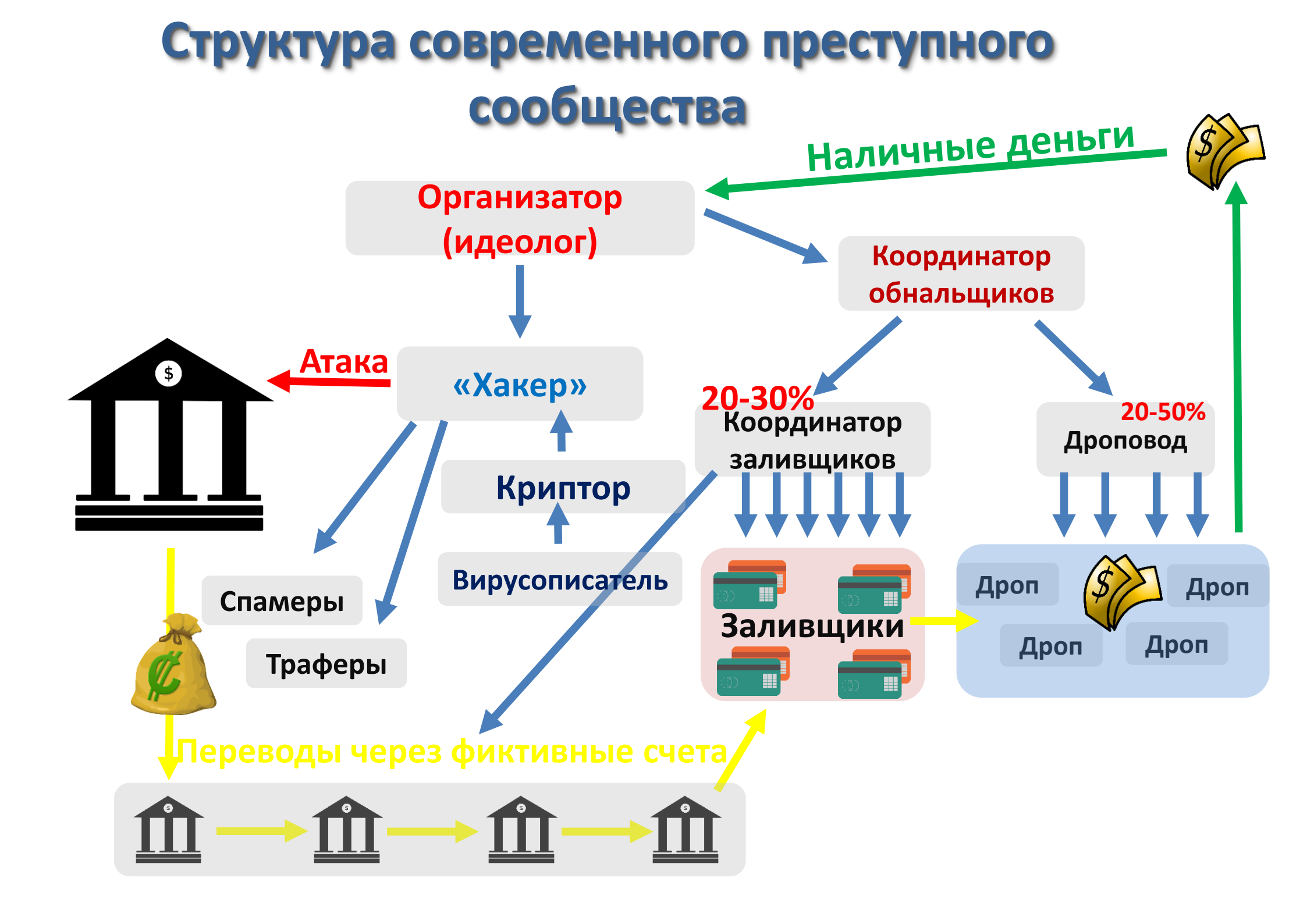
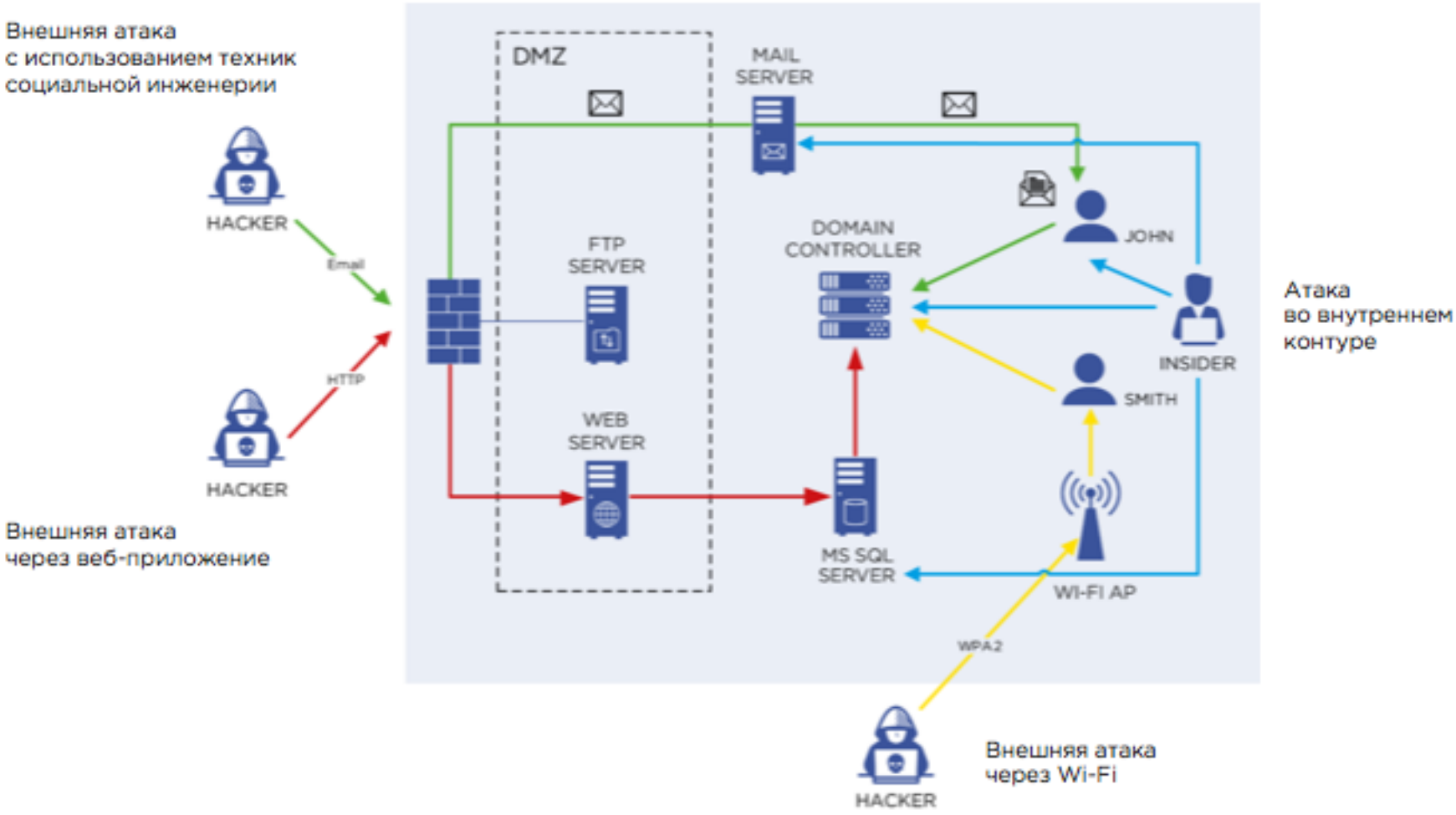


СХЕМА ВОЗМОЖНЫХ АТАК, ПРОИЗВОДИМЫХ ПРИ ПЕНТЕСТАХ



ВНЕШНИЙ ПЕНТЕСТ
И ТЕСТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ

- Поиск в интернете сайтов заказчика и поддоменов
- Сканирование портов и определение служб, использующих их
- Идентификация используемого ПО и технологий
- Поиск и анализ уязвимостей приложения, входящих в классификацию OWASP
- Проведение атак, направленных на эксплуатацию уязвимостей (по согласованию с заказчиком)
- Анализ результатов и подготовка рекомендаций

ВНУТРЕННИЙ ПЕНТЕСТ ИНФОРМАЦИОННЫХ СИСТЕМ

- Подключение к пользовательскому сегменту сети
- Анализ трафика протоколов канального и сетевого уровней
- Инструментальное сканирование ресурсов внутренней сети
- Поиск уязвимостей на обнаруженных ресурсах
- Проведение сетевых атак и атак, эксплуатирующих уязвимости
- Получение локальных и доменных учетных записей
- Анализ результатов и подготовка рекомендаций

ПЕНТЕСТ ТОЧЕК ДОСТУПА WI-FI

- Изучение характеристики и особенностей сетей Wi-Fi на объекте
- Проведение атак на аутентификацию и авторизацию в беспроводных сетях
- Получение ключей шифрования между клиентом и точкой доступа Wi-Fi
- Проведение атак на аппаратное обеспечение сетей Wi-Fi
- Установка поддельной точки доступа Wi-Fi, проведение атак на клиентов сетей
- Обработка результатов и подготовка рекомендаций

СОЦИОТЕХНИЧЕСКИЙ ПЕНТЕСТ

- Сбор данных об объекте и пользователях
- Подготовка провоцирующих данных
- Рассылка по электронной почте, целевое общение через соцсети и мессенджеры
- Личные звонки (телефон, Skype)
- Распространение носителей информации с провоцирующими данными
- Оценка преодоления физического периметра (скрытное копирование ключей СКУД)
- Анализ результатов и проведение обучения

ВНУТРЕННИЙ АУДИТ БЕЗОПАСНОСТИ

- Автоматизированная инвентаризация IT-активов
- Проверка актуальности версий ПО, ошибок конфигурации серверов и сетевого оборудования
- Поиск и анализ уязвимостей средств защиты
- Проверка соответствия стандартам ИБ (PCI DSS, NIST, NERC и др.)
- Анализ возможности проведения сетевых атак (Spoofing, MiTM)
- Построение векторов атак и подготовка плана для минимизации рисков ИБ

ПРИМЕР РЕАЛИЗАЦИИ

КОМПАНИЯ «А»:

5000
сотрудников

6
филиалов

160
B2B-клиентов
(крупных и средних
интернет-магазинов)

МЕРОПРИЯТИЯ:

Внешний пентест, включая
тестирование веб-приложений
методом «черного ящика»

СРОКИ:

25 рабочих дней

РЕЗУЛЬТАТЫ:

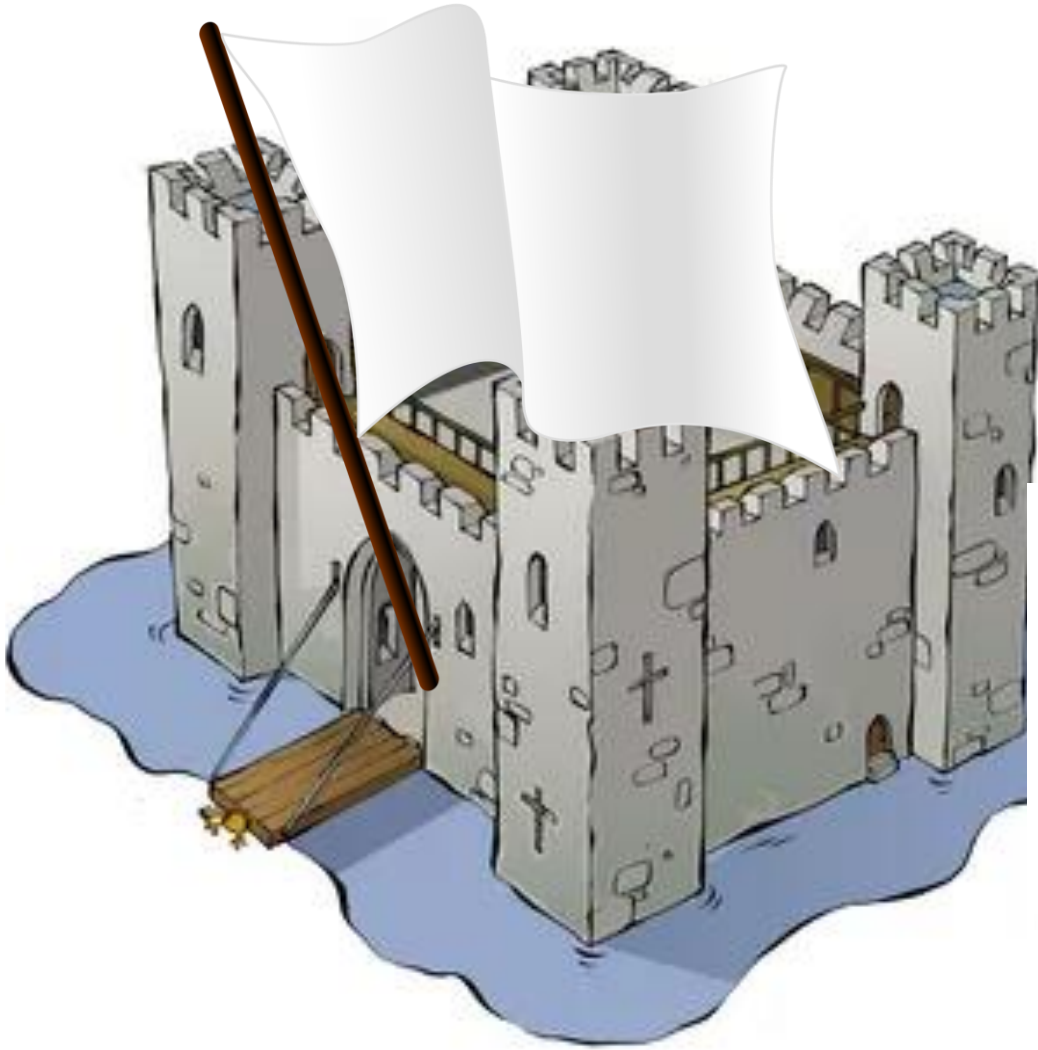
Выявлено 12 уязвимостей с низким уровнем риска,
5 – со средним, 2 – с высоким

Самая критичная уязвимость – SQL-инъекция
на веб-портале, которая позволяет злоумышленнику
получить контроль над сервером баз данных

Даны рекомендации, как повысить защищенность системы
с учетом всех выявленных уязвимостей

Традиционная концепция обеспечения ИБ

и ее минусы…



ТИПОВЫЕ УГРОЗЫ ДЛЯ БИЗНЕСА

01 | Репутационные риски, «черный» PR

02 | Санкционные и налоговые риски

03 | Невыполнение контрагентом/клиентом договорных обязательств

04 | Работа менеджмента и сотрудников против интересов компании

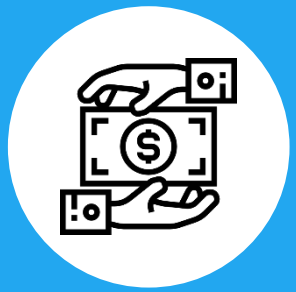
05 | Ущерб из-за утечек информации, нелигитимного доступа к данным, использования вредоносного ПО

06 | Мошенничество: присвоение и сокрытие активов, невозврат крупных кредитов, фишинг

ЧТО ТАКОЕ ETHIC

Сервис выявления мошеннических угроз для бизнеса

ETHIC:
External Threats
& Human Intelligence Center



Предотвращение нелегальных схем и утечек информации

Своего рода DLP-система, но работающая вне контура организации

Круглосуточный мониторинг в интернете

Отслеживание угроз в режиме 24/7

«Чтобы поймать преступника, нужно думать как преступник»

ПОРЯДОК РАБОТЫ СЕРВИСА

МОНИТОРИНГ

Автоматический анализ источников вне периметра компании: от соцсетей до ресурсов DarkNet

ОЦЕНКА

Аналитическая экспертиза уровня опасности
и определение тактики реагирования

ОПОВЕЩЕНИЕ

Отправка предупреждений
об угрозах для бизнеса
или инцидентах через специальный веб-портал

РЕАГИРОВАНИЕ

Блокировка источников, изменение технических
настроек сервисов,
проведение расследования

ИНСТРУМЕНТЫ ETHIC

01

DEEP SOCIAL NETWORK ANALYSIS

Мониторинг и глубокий анализ данных социальных сетей

02

DARKWEB & TELEGRAM SEARCH

Архивирование и анализ ресурсов «теневого» интернета

03

MARKETSCAN

Поиск на торговых площадках индикаторов мошенничества в отношении компании

04

PHISHING RADAR

Выявление ресурсов фишинга или целевой атаки (от сайтов до мобильных приложений)

05

PUBLIC LEAKS DATABASE

Мониторинг и анализ публичных утечек данных

06

KNOWLEDGE BASE OF THREATS

База знаний угроз — источник данных и скоринг-моделей

07

READY-TO-QUIT

Выявление сотрудников, готовящихся к увольнению

08

LEGAL RISK ALERT

Мониторинг юридически значимых опасных событий в деятельности контрагентов

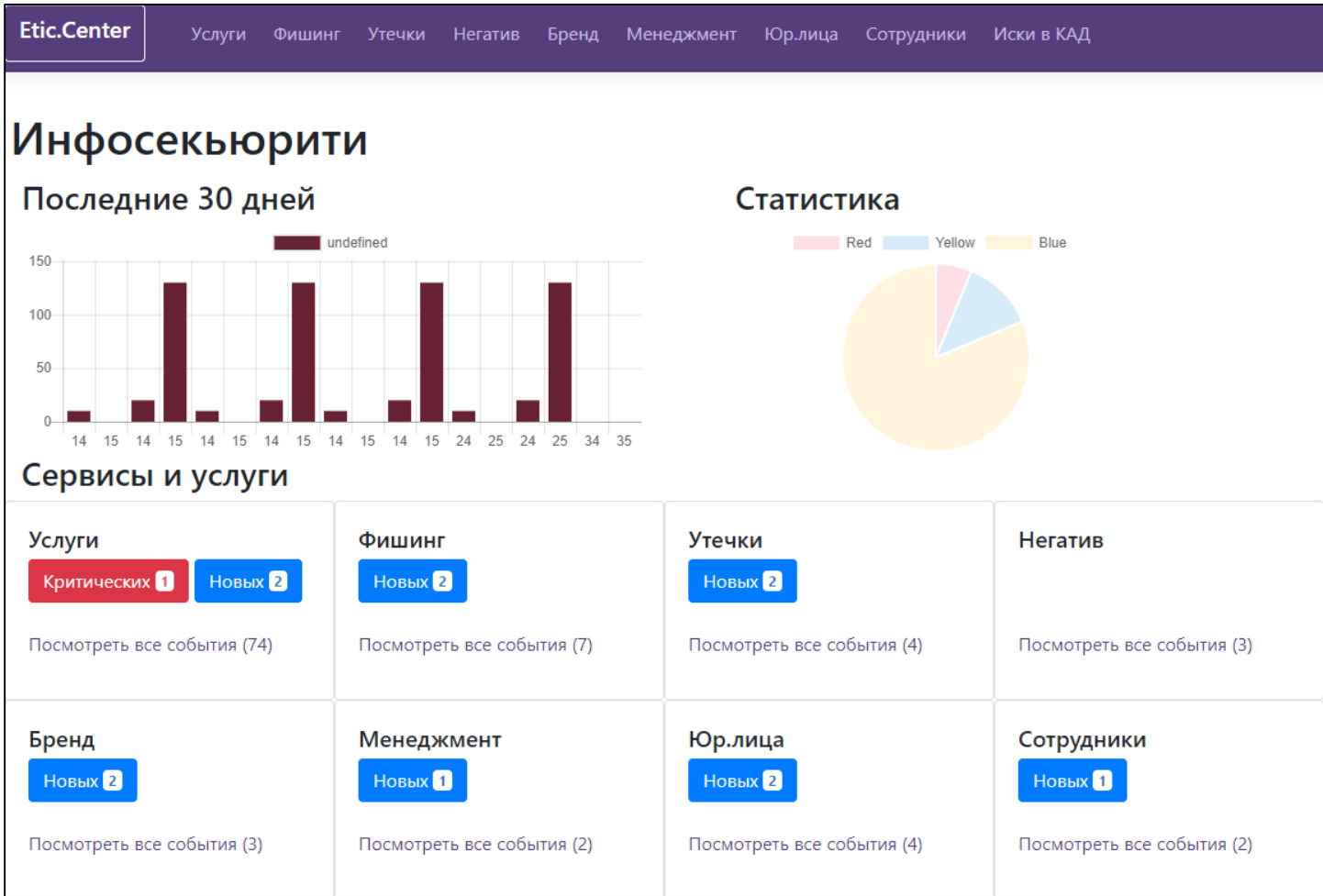
ИСТОЧНИКИ ETHIC

ПОРТАЛ ETHIC

Портал ETHIC содержит детальную информацию по каждому событию: ссылки, тексты, имена авторов, риски, рекомендации, предпринятые действия и т.д.

Профили помогут отслеживать активность и соединять различные угрозы распространенные одним фигурантом

.



КЕЙС «PR-АТАКА»

Выявленные события: благодаря сервису найден сайт и два сообщества в соцсетях, публикующие ложные негативные материалы о крупном объекте строительства. Застройщик несет убытки в виде недополученной прибыли.

Сумма предотвращенного ущерба: не известна.

РАБОТЫ

Оповещена служба безопасности

Домен и группы поставлены на контроль

При дальнейшем проведении расследования установлены организаторы и исполнители атаки

Приняты меры по блокировке ресурсов

РЕЗУЛЬТАТЫ

Ресурс и группы в соцсетях заблокированы

Восстановлен поток клиентов, готовых приобрести недвижимость у застройщика

Сохранена репутация компании и ее руководства

КЕЙС «ПРОДАЖА КОНТРАФАКТА»

Выявленные события: в соцсети обнаружена публикация о продаже крупных партий контрафактной продукции известного производителя одежды. Компания несет репутиционные потери и убытки в виде недополученной прибыли.

Сумма предотвращенного ущерба: >50 млн руб.

РАБОТЫ

Оповещена служба безопасности

Получены дополнительные сведения от продавца (количество продукции, стоимость, сроки, адреса)

Собраны контактные данные продавца

Выявлены аналогичные предложения на других торговых площадках (>30 фактов)

РЕЗУЛЬТАТЫ

Установлен и закрыт канал сбыта

Минимизированы репутационные и финансовые потери

Совместно с правоохранительными органами конфисковано контрафактной продукции на сумму более 10 млн рублей

КЕЙС «ОБЪЯВЛЕНИЕ В DARKNET»

Выявленные события: на околокриминальном ресурсе DarkNet обнаружена публикация о поиске «дропов» со счетами в защищаемом банке. Клиент может понести многомиллионные убытки от нелегальных финансовых операций.

Сумма предотвращенного ущерба: >300 млн руб.

РАБОТЫ

Оповещена служба безопасности

Получены дополнительные сведения об авторе

Принято участие в расследовании инцидента

РЕЗУЛЬТАТЫ

Выявлена попытка несанкционированного вывода из банка 320 млн руб.

Установлены организаторы и исполнители хищения

Заблокированы банковские счета с денежными средствами на общую сумму более 17 млн руб.

ПРЕИМУЩЕСТВА ETHIC

Комплексный подход:
объединенная информация
из важных для Заказчика источников

Постоянный мониторинг:
автоматизированная проверка
по специальным алгоритмам

Учет специфики:
персональный аналитик анализирует
события, погружаясь в проблематику
Заказчика и отрасль

Уникальные объекты мониторинга:
рекламные объявления, открытые
файлообменники, аккаунты
в соцсетях и т.д.


INFOSECURITY
AWARENESS:
ОБУЧЕНИЕ
ПО ВОПРОСАМ ИБ

Все совершают ошибки

От невнимательности

От незнания

Социальная инженерия

Социальная инженерия

СТАТИСТИКА

Согласно данным статистики, 2/3 инцидентов ИБ являются результатом действий сотрудников компании.

40% компаний

не имеют стратегии информационной безопасности

56% компаний

не имеют разработанного процесса реагирования на инциденты

48% компаний

не имеют программы обучения нормам и требованиям ИБ

* данные PWC по итогам опроса 248 российских компаний в 2017 году

КОМПЛЕКСНЫЙ ПОДХОД

Мы анализируем текущее состояние осведомленности об угрозах ИБ,
а затем организуем комплексное обучение сотрудников компании.

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ ПО ВОПРОСАМ ИБ

Очное обучение

Дистанционное обучение

Контроль эффективности

Дополнительные материалы

Отчетность по сервису

ОЧНОЕ ОБУЧЕНИЕ

Теоретическая информация усваивается лучше, когда ее подача сопровождается живым общением.

Тренинги

Семинары

Вы можете выбрать тему из нашей базы или предложить собственную

Занятия проводятся в том числе с применением кейс-метода

По итогам занятия обучающимся предлагается пройти тестирование

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ

Сотрудники могут пройти полное обучение в удобное для них время, не покидая рабочего места.

Электронные курсы

Видеоролики GoAnimate

Рассылки Security Tips

Вебинары

Обучение проводится по модульному принципу (гибкая комплектация материалов)

Мы уделяем основное внимание практическим вопросам, конкретным кейсам и проблемам

Наши учебные материалы можно просматривать на разных типах электронных устройств

ЭЛЕКТРОННЫЕ КУРСЫ

Для разработки курсов мы используем профессиональный комплекс программ Articulate 360. Готовые курсы упаковываются в стандартный SCORM-пакет.

МИРОВЫЕ ТРЕНДЫ

ПЕРСОНАЛИЗАЦИЯ

ГЕЙМИФИКАЦИЯ

МИКРООБУЧЕНИЕ

Возможно создание обучающих курсов в Microsoft PowerPoint.

КОНТРОЛЬ ЭФФЕКТИВНОСТИ

Эффективность обучения анализируется и отражается
в конкретных количественных показателях.

**Тестирования,
упражнения и кейсы**

Образовательные игры

**Учебные фишинговые
рассылки**

Пользователи закрепляют полученные знания
в классической или альтернативной форме

Все проверочные материалы готовятся
с учетом сферы вашей деятельности

По результатам контроля эффективности
предоставляется детальная отчетность

ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ

Текстовые и графические материалы делают обучение более разнообразным и запоминающимся.

Памятки и брошюры

Карточки и лонгриды

Плакаты

Скринсейверы

Стикеры

К разработке контента привлекаются профессиональные дизайнеры и иллюстраторы

Мы готовим уникальные текстовые материалы или предоставляем качественный рерайт

Вы сами устанавливаете периодичность размещения обучающего контента

ИНДИВИДУАЛЬНАЯ ПРОГРАММА ОБУЧЕНИЯ

Пакет материалов составляется с учетом конкретных задач обучения и целевой аудитории (возраст, должность, опыт работы и т.п.).

Обучение новых сотрудников

Начальные знания

Базовые навыки

Обучение действующих сотрудников

Новые методики, стандарты, формы, программы, системы

Изменения в бизнес-процессах компании

Повышение квалификации

Конкретные темы, направления, области, компетенции

ЭТАПЫ

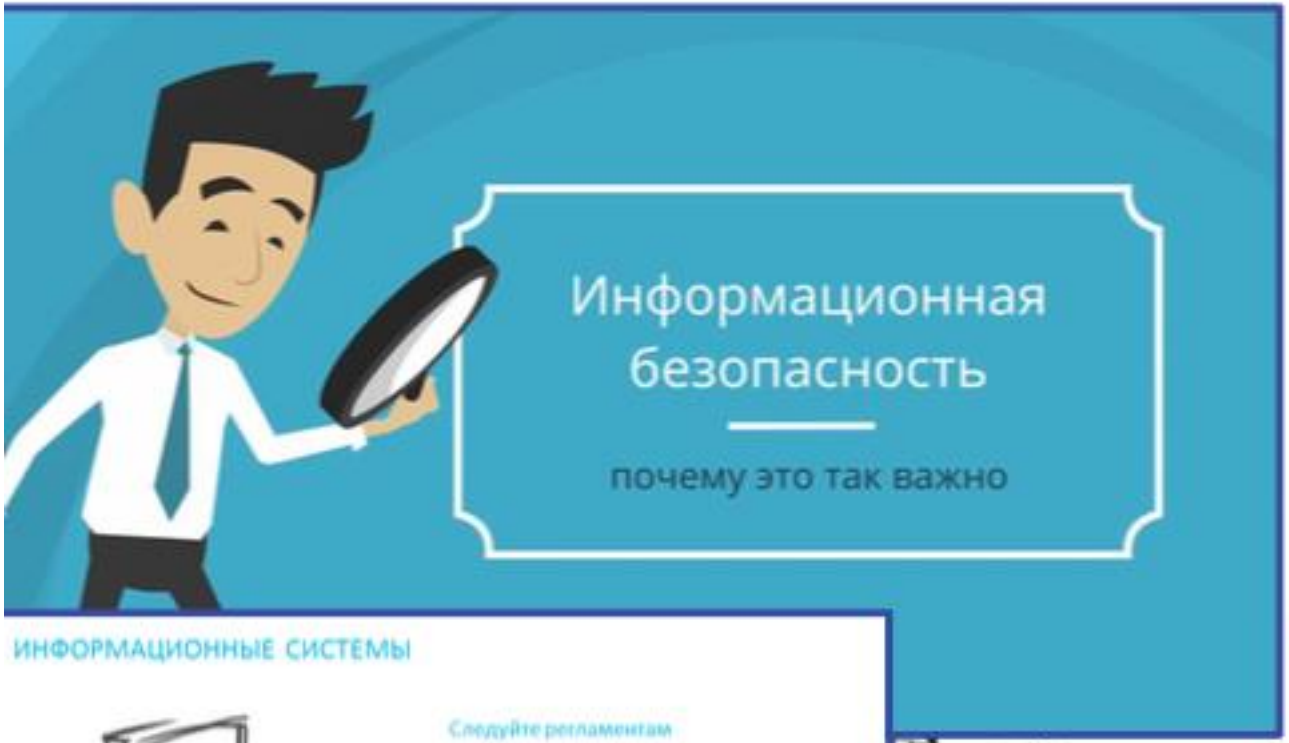
1 ОПРЕДЕЛЯЕМ ЦЕЛЕВУЮ АУДИТОРИЮ

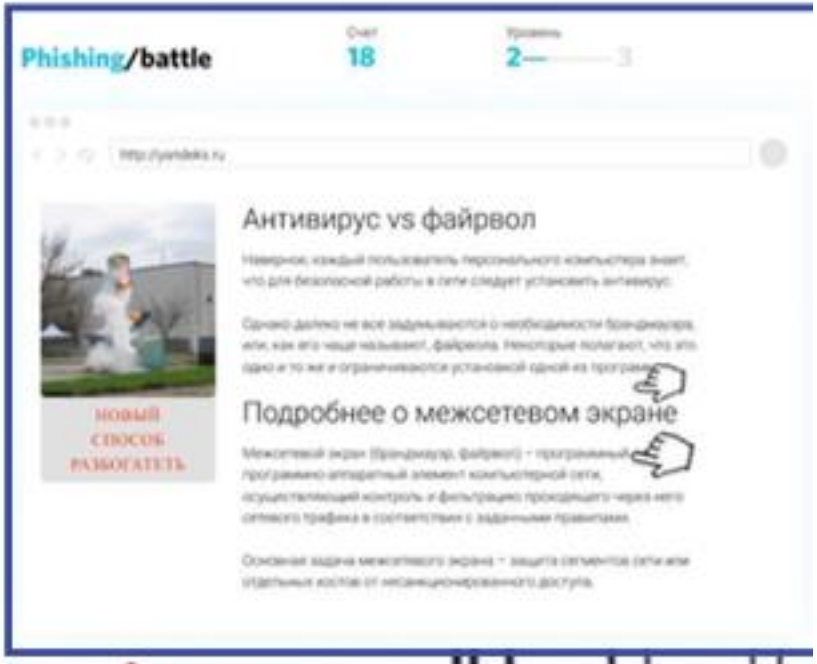
2 ГОТОВИМ И СОГЛАСУЕМ ОБУЧАЮЩИЙ КОНТЕНТ

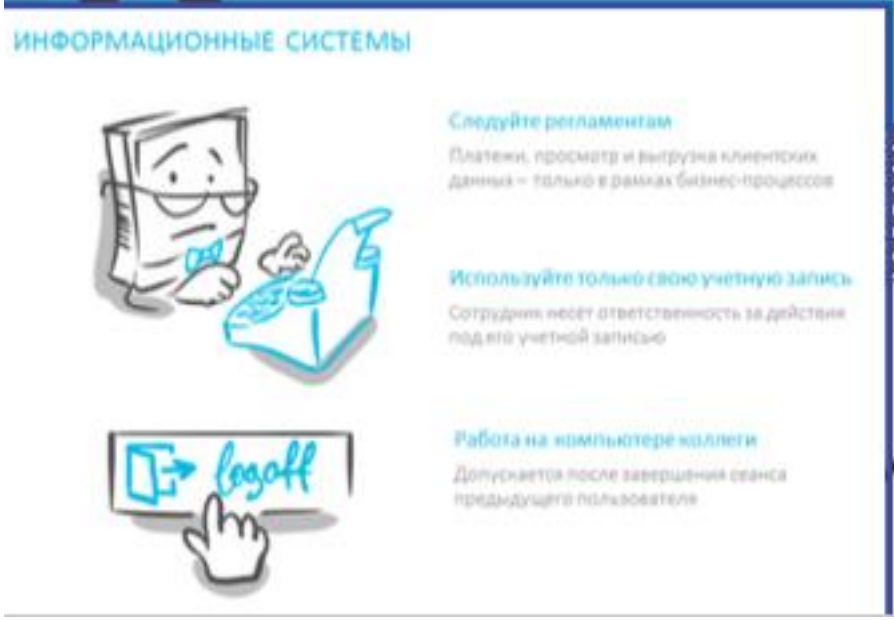
3 ПРОВОДИМ ОБУЧЕНИЕ

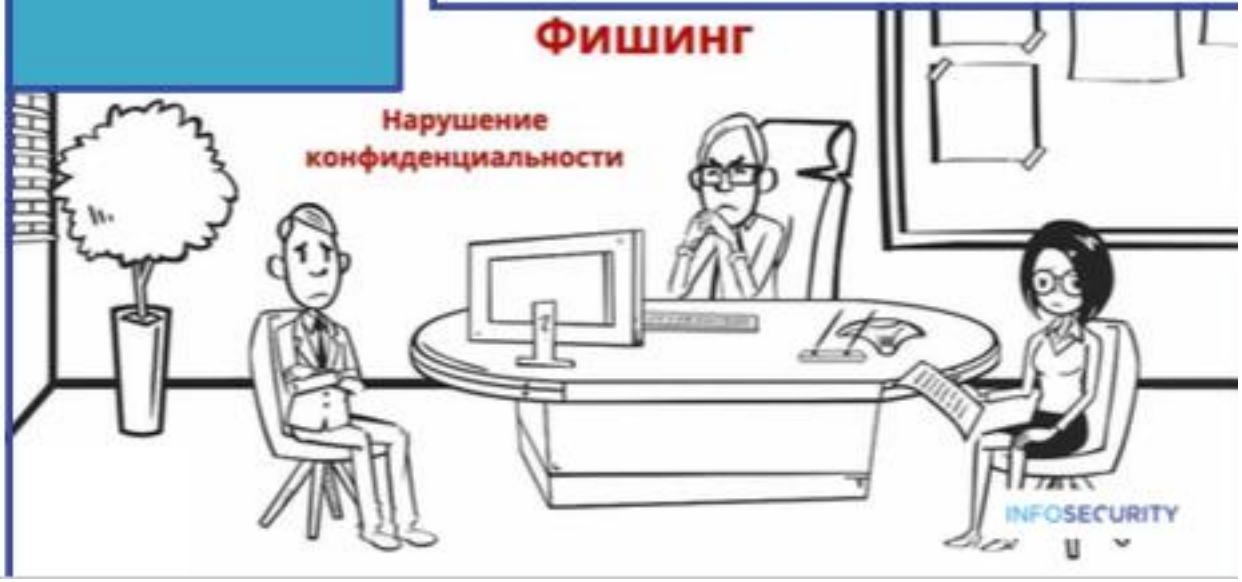
4 ПОЛУЧАЕМ ОБРАТНУЮ СВЯЗЬ И ДОРАБАТЫВАЕМ КОНТЕНТ

ПРИМЕРЫ ОБУЧАЮЩИХ МАТЕРИАЛОВ

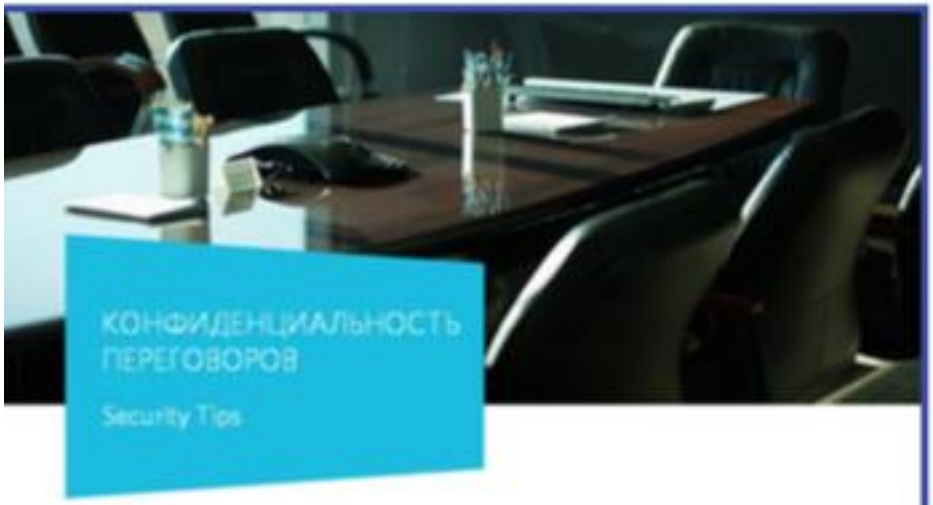








ПРИМЕРЫ ОБУЧАЮЩИХ МАТЕРИАЛОВ



В этом выпуске Security Tips мы расскажем о правилах безопасного обсуждения рабочих вопросов и о том, почему эти правила важно соблюдать.

ЗАЩИЩАЙТЕ ИНФОРМАЦИЮ

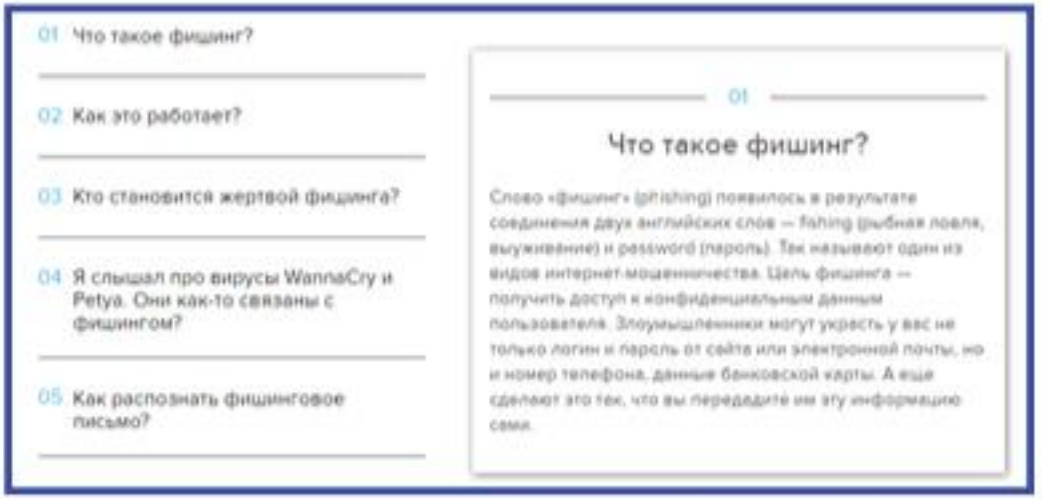
Задумываетесь ли вы о безопасности конфиденциальной информации, когда обсуждаете с коллегами рабочие моменты в опен спейсе, лифте, кафе или на парковке? Бронируете ли переговорную комнату, если предстоит важный деловой разговор? Представляете ли, что может стать результатом случайно подслушанной фразы?

Последствия разглашения конфиденциальной информации могут быть действительно серьезными. Для Компании это потеря конкурентных преимуществ и клиентов, санкции со стороны регулирующих органов, утрата деловой репутации. Для сотрудника, допустившего разглашение, — ухудшение атмосферы в коллективе, денежный штраф, выговор или даже увольнение. Чтобы избежать этих неприятностей, достаточно следовать рекомендациям Службы ИБ.

ВЕДИТЕ ПЕРЕГОВОРЫ ПРАВИЛЬНО

Не устраивайте совещаний в кафе или столовой

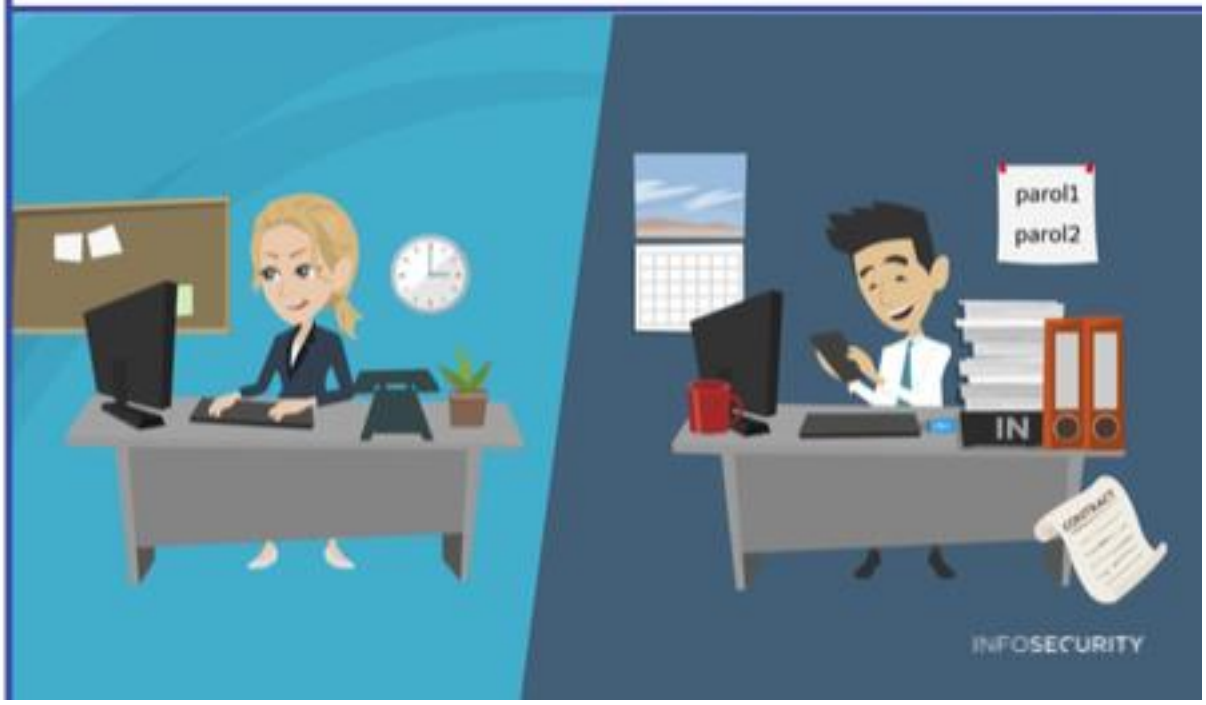
Если вы вынуждены обсуждать рабочие процессы во время обеденного перерыва, постарайтесь, чтобы сидящие рядом люди не стали невольными слушателями ваших переговоров. Старайтесь говорить тише, особенно если этого требует характер обсуждаемой информации. Следите за тем, чтобы не допустить разглашения персональных данных своих коллег — например, размера их заработной платы.



01

Что такое фишинг?

Слово «фишинг» (phishing) появилось в результате соединения двух английских слов — fishing (рыбная ловля, выуживание) и password (пароль). Так называют один из видов интернет-мошенничества. Цель фишинга — получить доступ к конфиденциальным данным пользователя. Злоумышленники могут украсть у вас не только логин и пароль от сайта или электронной почты, но и номер телефона, данные банковской карты. А еще сделают это так, что вы передадите им эту информацию сами.



БАЗОВЫЙ НАБОР ТЕМ ОБУЧЕНИЯ

- Конфиденциальная информация и правила работы с ней
- Место ИБ в бизнес-процессах компании
- Информационная безопасность на рабочем месте
- Информационная безопасность при удаленной работе
- Уменьшение рисков информационной безопасности
- Персональные данные: понятие, обработка, защита
- Программно-технические средства обеспечения ИБ
- Криптография: базовые знания о науке шифрования
- Социальная инженерия: способы борьбы с мошенниками
- Законодательная и нормативно-правовая база ИБ

НАШИ ПРЕИМУЩЕСТВА

Мы гарантируем действительно эффективное обучение по вопросам информационной безопасности.

Повышаем осведомленность в сфере ИБ в различных формах по выбранным каналам

СИСТЕМНОСТЬ

Разрабатываем обучающий контент с учетом вашего фирменного стиля (согласно брендбуку)

КРЕАТИВНОСТЬ

Излагаем учебный материал простым и понятным языком независимо от выбранной темы

ДОСТУПНОСТЬ

gk-is.ru