Учения по Кибербезопасности

Когда проводить?
Как автоматизировать?
Что мы получаем в результате?

Прокопов Максим Дмитриевич
Руководитель направления ИБ

+7 (383) 255-3-255
pmd@axxtel.ru
axxtel.ru

БАЗОВАЯ ГОТОВНОСТЬ

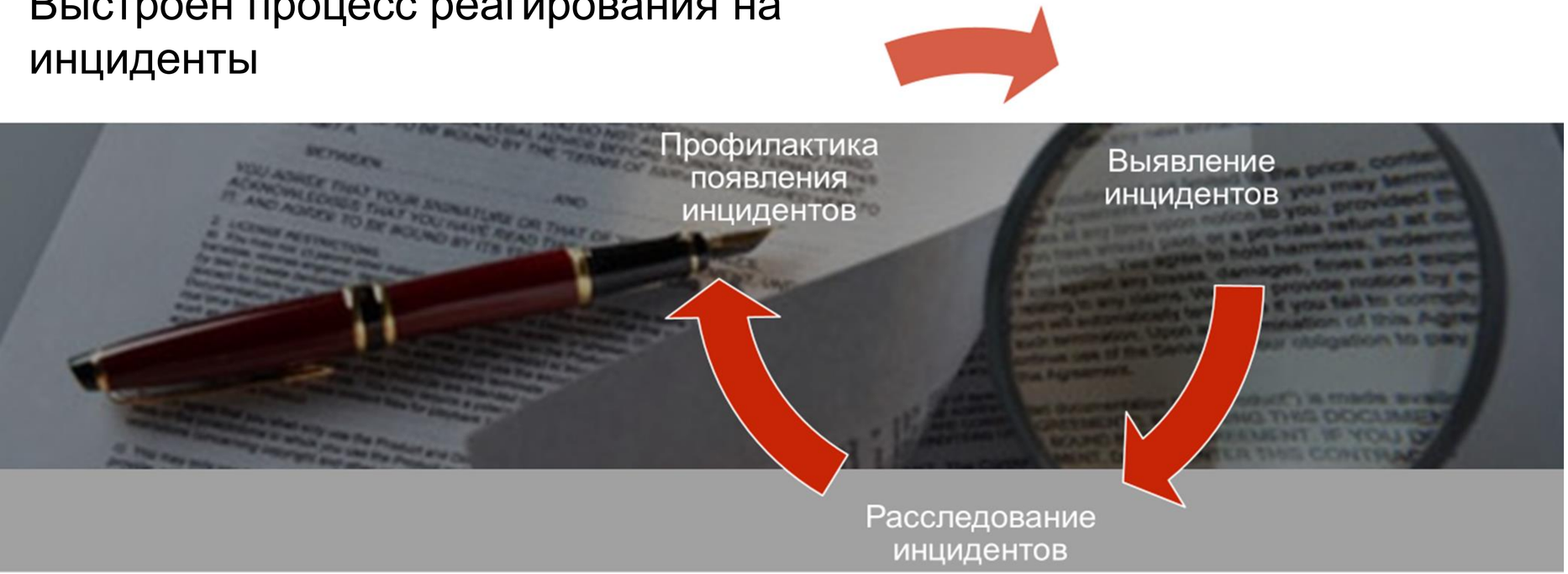
Внутренние инциденты

Внешние инциденты

Осведомленность персонала (по льзователи и специалисты)

КОГДА ПРОВОДИТЬ КИБЕРУЧЕНИЯ?

Выстроен процесс реагирования на инциденты



Его работу необходимо проверять и отлаживать по каждой подсистеме информационной безопасности.

1 НЕДОПУСТИТЬ ПОЯВЛЕНИЯ НОВЫХ ИНЦИДЕНТОВ

2 ОПЕРАТИВНО ВЫЯВЛЯТЬ ИНЦИДЕНТЫ

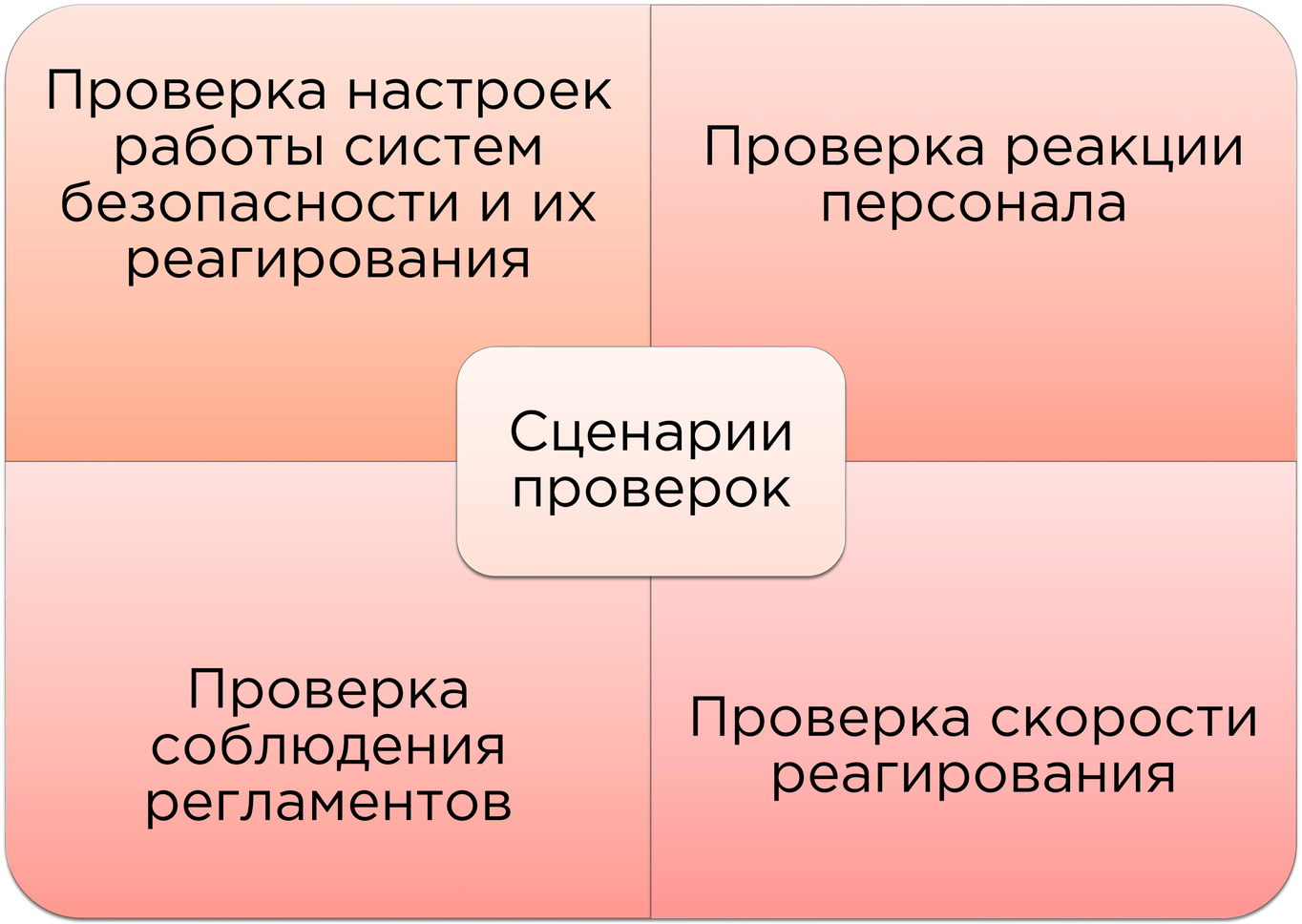
3 МИНИМИЗИРОВАТЬ РИСКИ ОТ СВЕРШЕННЫХ ИНЦИДЕНТОВ

Не стоит учится на реальных инцидентах

ОСНОВНЫЕ НАПРАВЛЕНИЯ

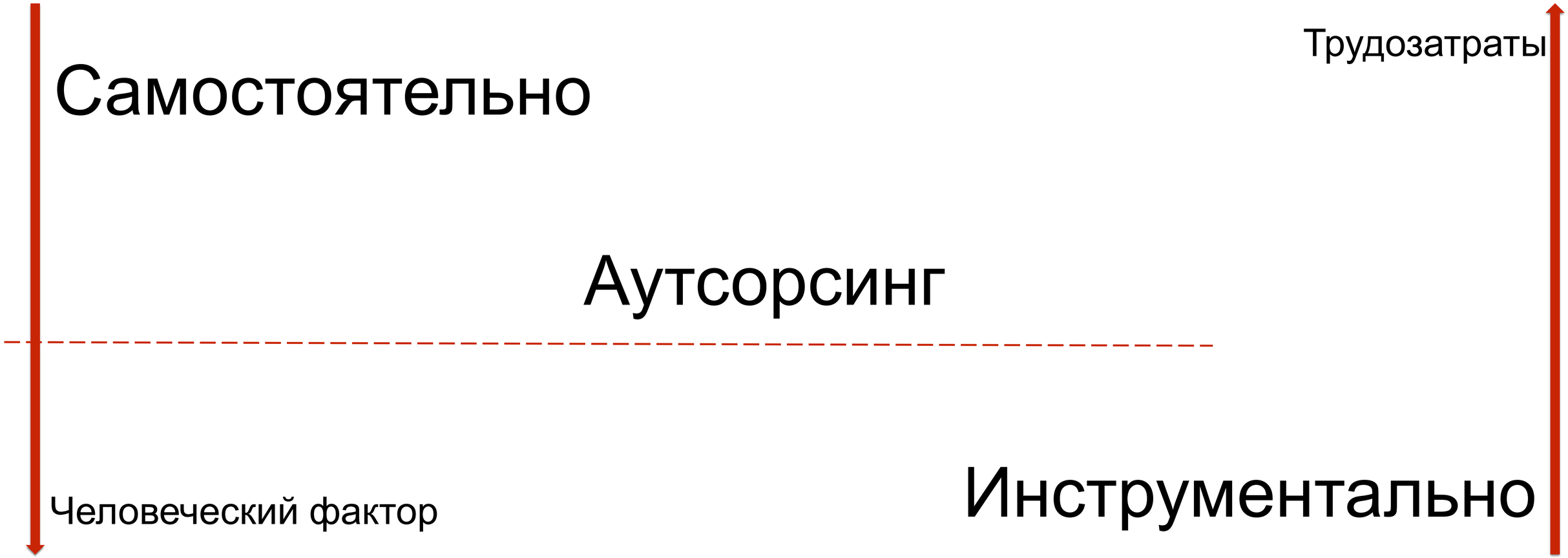
Какой метод выбрать?

ХАРАКТЕРИСТИКИ ПРОВЕРОК



- Минимальные трудозатраты
- Максимальная площадь покрытия
- Уход от человеческого фактора
- Независимая оценка
- Проверка по утвержденным показателям

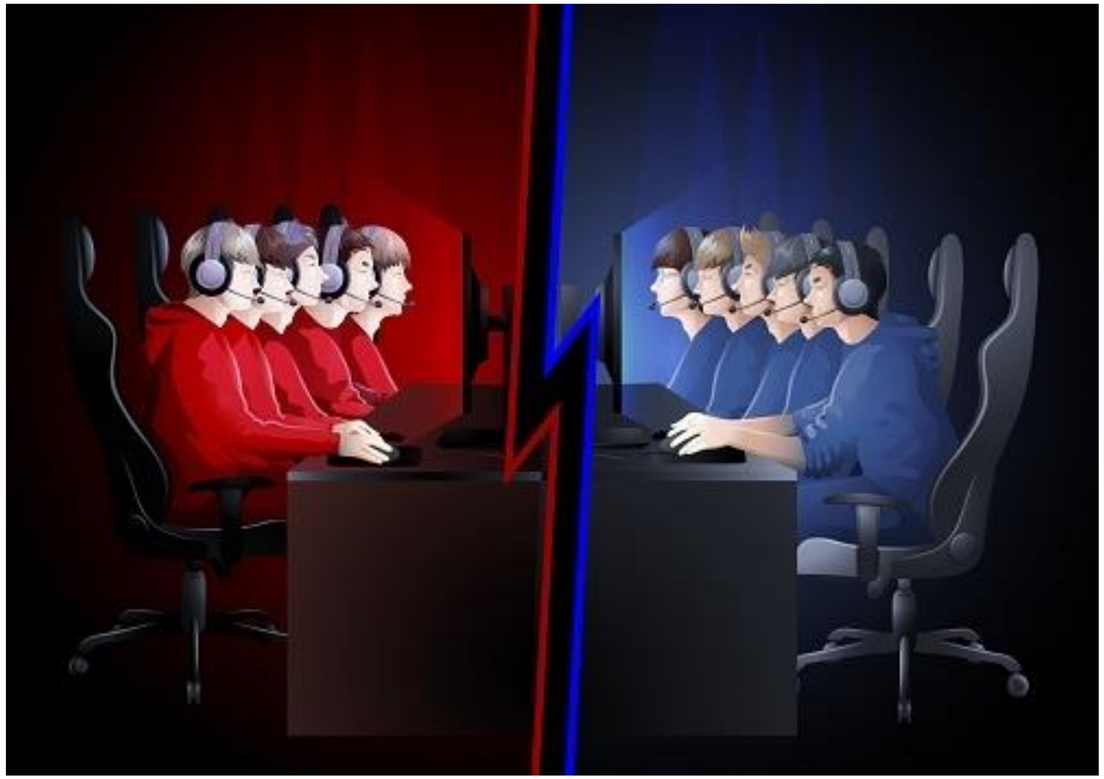
НЕОБХОДИМОСТЬ ПРОВЕРКИ



ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

1. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
2. ВЗЛОМ ПЕРИМЕТРА СЕТИ
3. ВЗЛОМ САЙТА
4. ВЗЛОМ ВНУТРЕННЕГО ПЕРИМЕТРА
5. ВЗЛОМ WI-FI
6. ПРИЛОЖЕНИЯ

Черный ящик
Серый ящик
До достижения цели
Физическое проникновение



Red team & Blue team

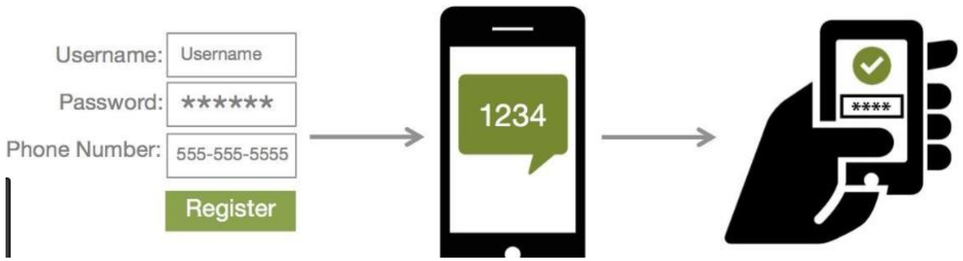
АВТОМАТИЗАЦИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ

SkyBox

Pentera

Cymulate

СТОЙКОСТЬ ПАРОЛЕЙ



Аудит паролей корпоративной инфраструктуры, аудит подсистем усиленной аутентификации

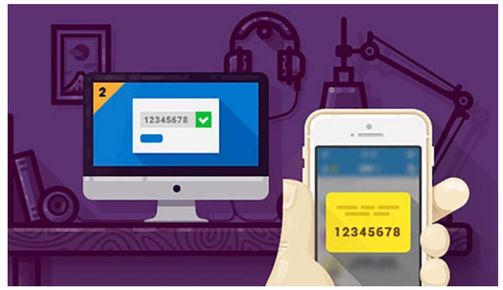
SPECOPS

Password Policy
(Информационная безопасность)

Расширяет возможности парольной политики AD. Позволяет:
- Создавать парольные словари
- Запрещать использование имен, дат рождения, названия городов и т.д.
- Настраивать частоту смены пароля в зависимости от его сложности
- Создавать информативные пользовательские сообщения
- Запрещать к использованию части логинов, номера компьютеров
- Уведомлять об истечении срока действия пароля по эл. почте

Specops Blacklist
(Информационная безопасность)

Исключает использование пользователями скомпрометированных паролей в различных ресурсах сети интернет, которые могут использоваться злоумышленниками при брутфорсе. Вариант использования:
- локальное исполнение
- в облаке



Microsoft Azure

axxtel

КОНТРОЛЬ СОТРУДНИКОВ

Проведение аудита системы

- Доработка правил
- Аудит инцидентов
- Отчет

Имитация действий внутреннего нарушителя

- Имитация утечки
- Имитация сотрудника в зоне риска
- Имитация нарушения трудового распорядка

ФИШИНГ

САИБ

Рассылки

Сценарии	Написание остросоциальных сценариев, связанных с деятельностью организации
Формы авторизации	Верстка форм авторизации любой сложности
Полезная нагрузка	Создание псевдо-вирусных вложений, которые собирают данные пользователей.
Отчетность	Формирование полного отчета о проведенной рассылки: дата, время, факты открытия, перехода, активации, отправленные данные.
Доказательная база	Полученные данные можно использовать для формирования доказательной базы.

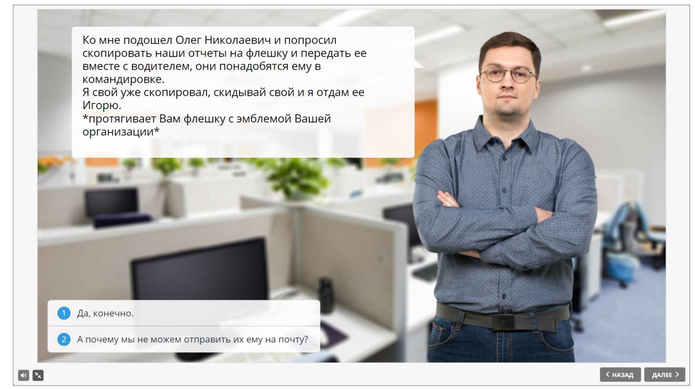
Обход системы безопасности

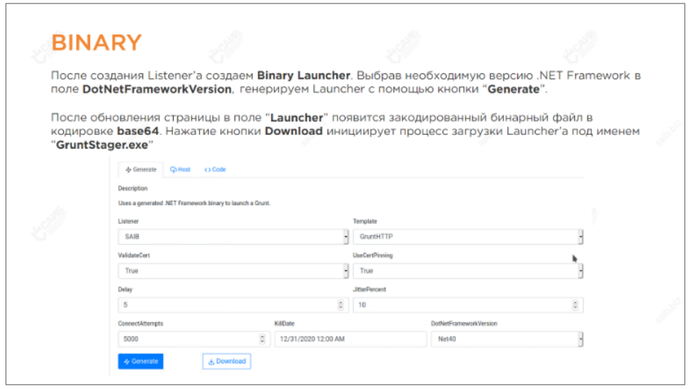
AV/EDR	Обфускация кода, использование тактик "Living off the Land"
Sandbox	Детектирование виртуализации, установленного ПО для мониторинга, анализ эмуляции работы пользователя
Шлюз безопасности почты, Антиспам	Повышение доверия доменов, организация ссылок с помощью облачных хранилищ, проверка возможности подмены отправителя, использование небинарных загрузчиков вредоносного кода, упаковщиков/архивов
IDS/IPS	Использование легитимных протоколов для управления агентом, изменение поведения эксплойтов и агентов в сети
DPI, Web-фильтрация	Инкапсуляция трафика с использованием ряда легитимных протоколов и служб/сервисов в сети Интернет

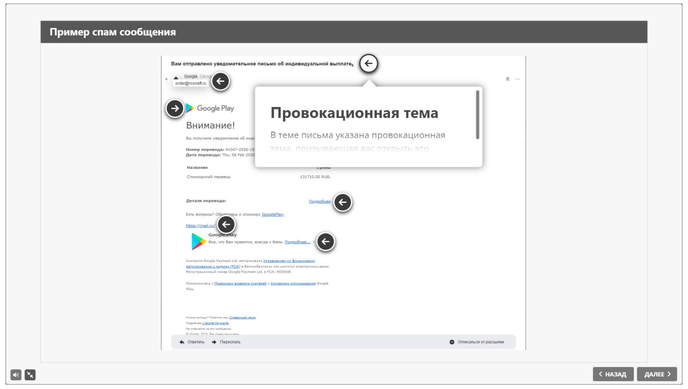
КАК НАУЧИТЬ СОТРУДНИКОВ БОРОТЬСЯ СО ЗЛОУМЫШЛЕННИКАМИ?

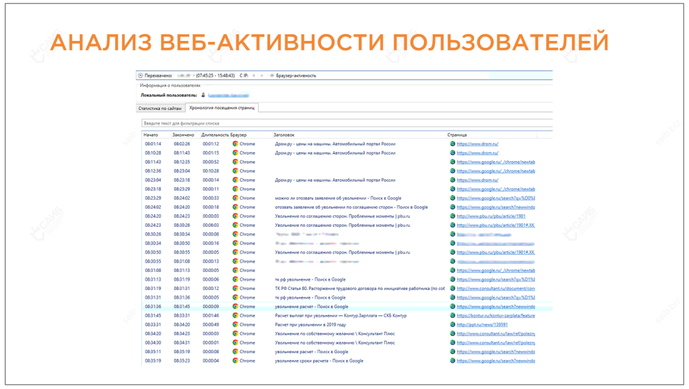
САИБ

- Повышение осведомленности пользователей;
- Востребованность персонализированных учебных материалов;
- Проведение периодических кибер-учений;
- Разбор основных ошибок пользователей по итогам фишинговых рассылок;
- Повышение квалификации инженеров (регламент реагирования).









НАШИ КОМПЕТЕНЦИИ

Более 700 реализованных проектов

Более 30 успешных проектов с компаниями списка РБК ТОП-500

20 специалистов направления

Опыт комплексных проектов под ключ

В наличии необходимые и сопутствующие лицензии

НАШИ КЛИЕНТЫ

Спасибо за внимание

ВАШИ ВОПРОСЫ

SKYPE: MAKSIM_PROKOPOV

EMAIL: PMD@AXXTEL.RU

Презентацию можно получить по запросу на info@axxtel.ru