

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

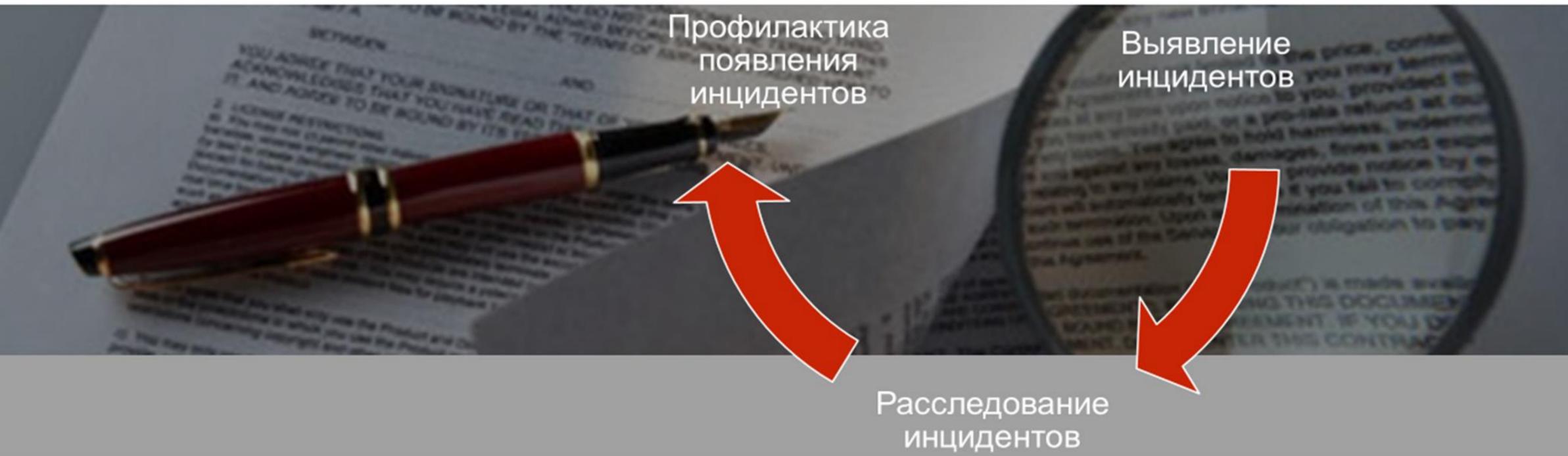


Осведомленность персонала (пользователи и специалисты)



КОГДА ПРОВОДИТЬ КИБЕРУЧЕНИЯ?

Выстроен процесс реагирования на инциденты



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

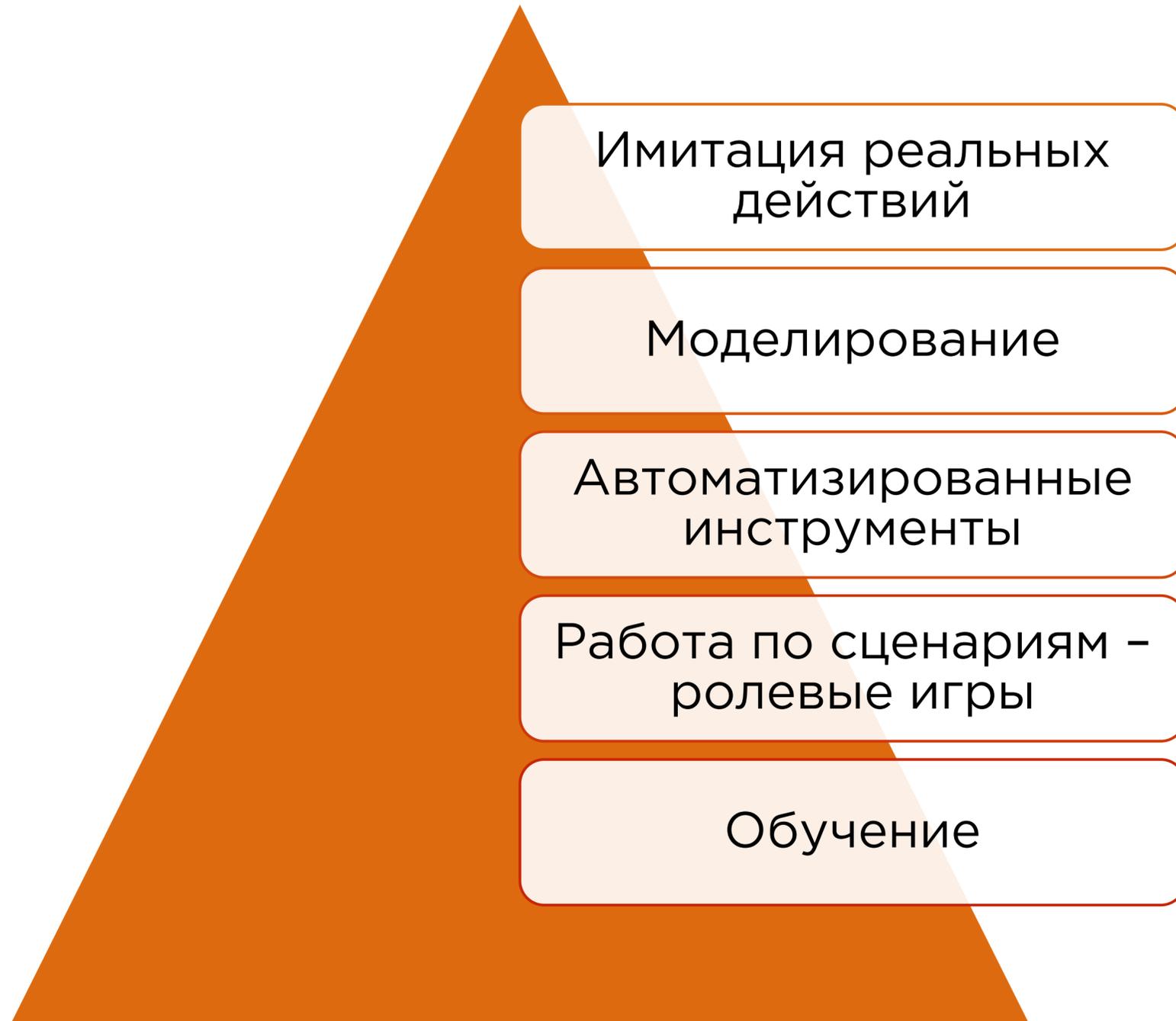
1 НЕДОПУСТИТЬ ПОЯВЛЕНИЯ НОВЫХ ИНЦИДЕНТОВ

2 ОПЕРАТИВНО ВЫЯВЛЯТЬ ИНЦИДЕНТЫ

3 МИНИМИЗИРОВАТЬ РИСКИ ОТ СВЕРШЕННЫХ ИНЦИДЕНТОВ

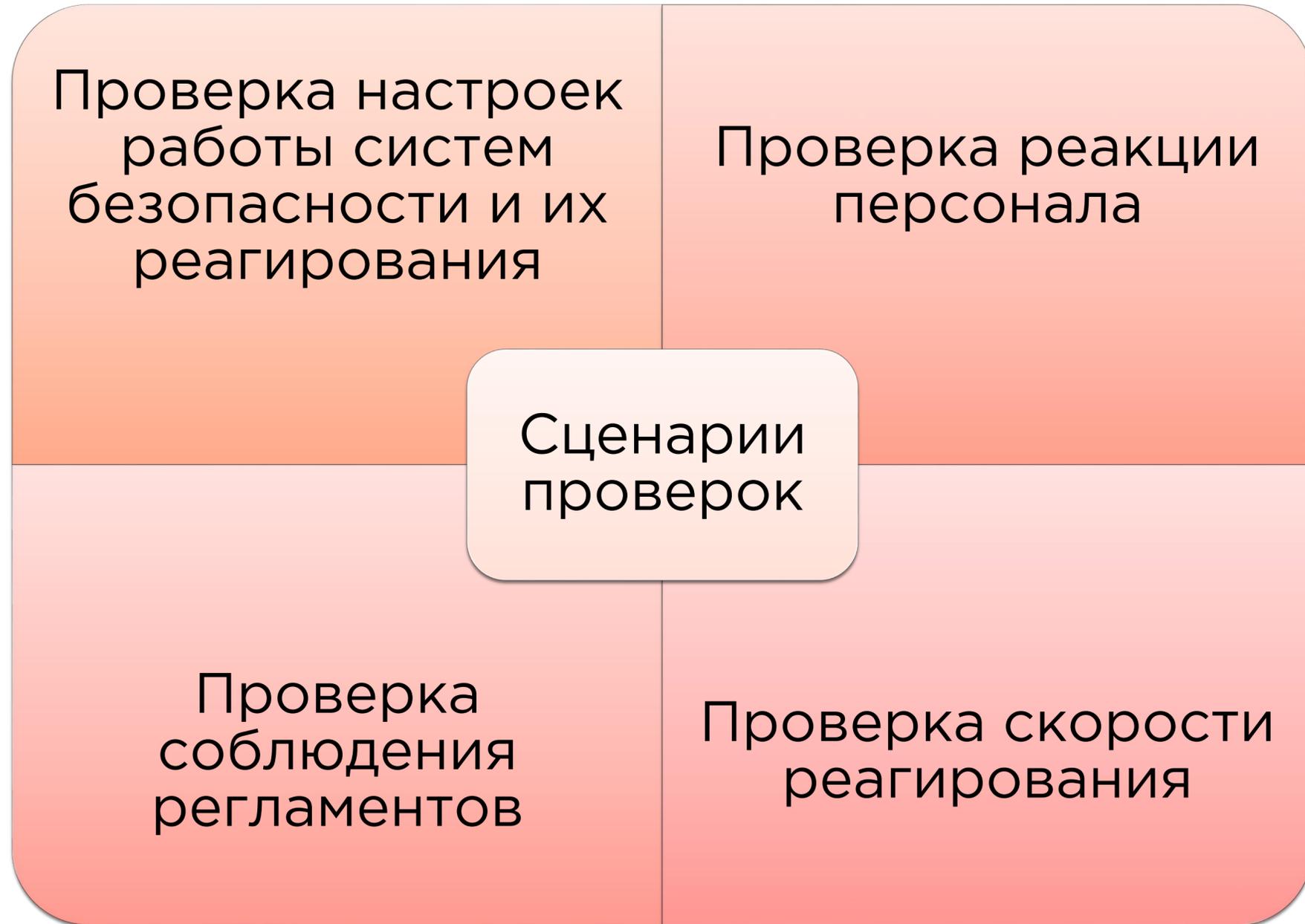
Не стоит учиться на реальных инцидентах

ОСНОВНЫЕ НАПРАВЛЕНИЯ



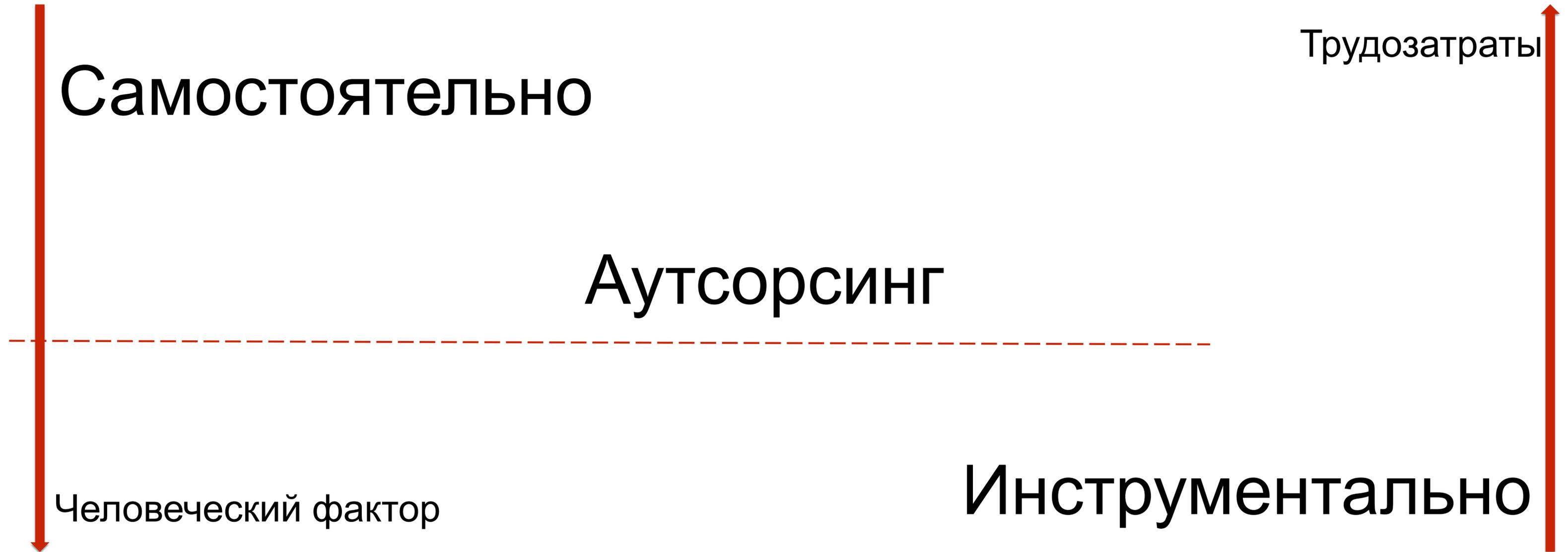
Какой метод выбрать?

ХАРАКТЕРИСТИКИ ПРОВЕРОК



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

НЕОБХОДИМОСТЬ ПРОВЕРКИ



ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

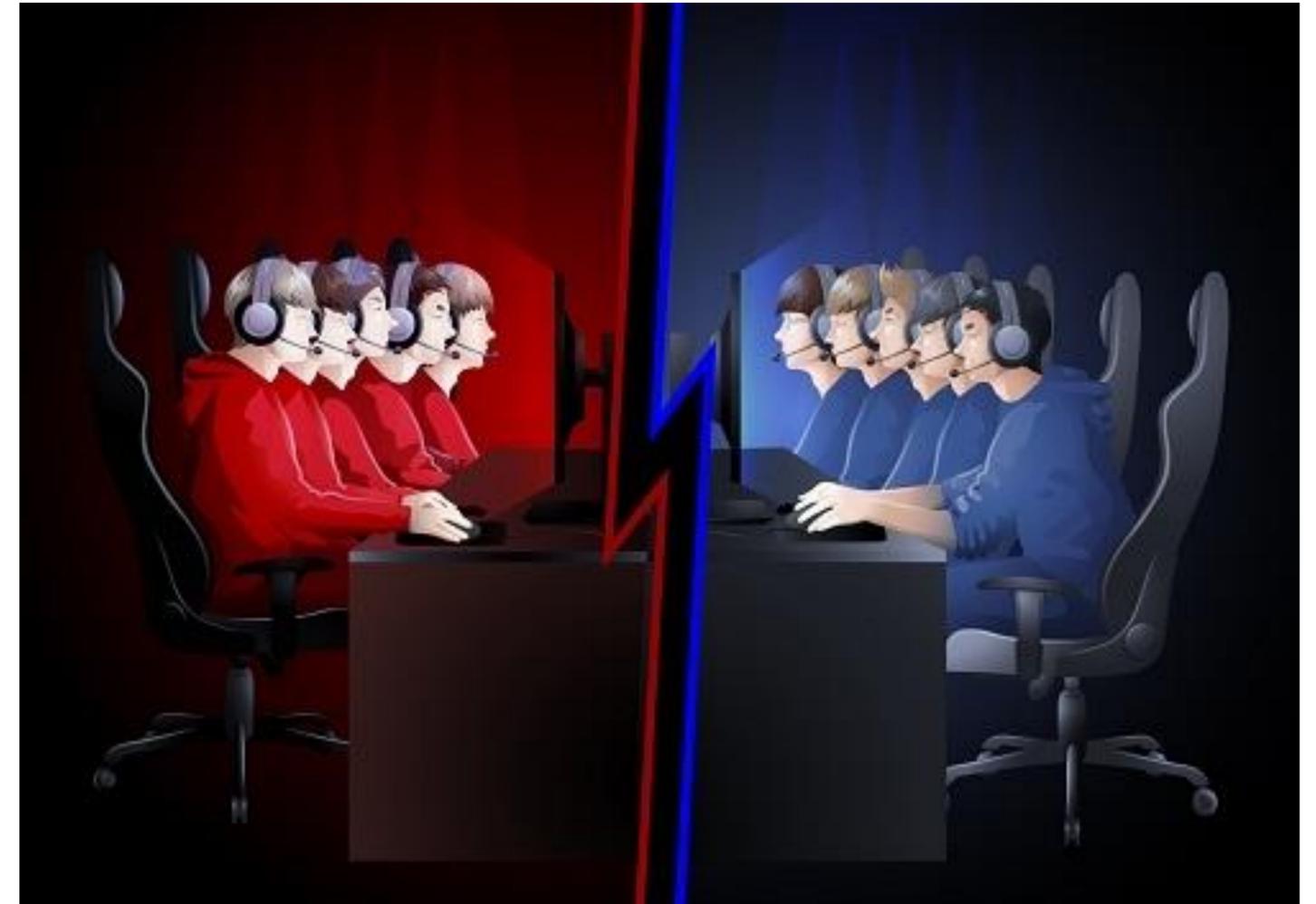
1. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
2. ВЗЛОМ ПЕРИМЕТРА СЕТИ
3. ВЗЛОМ САЙТА
4. ВЗЛОМ ВНУТРЕННЕГО ПЕРИМЕТРА
5. ВЗЛОМ WI-FI
6. ПРИЛОЖЕНИЯ

Черный ящик

Серый ящик

До достижения цели

Физическое проникновение



Red team & Blue team

АВТОМАТИЗАЦИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ

SkyBox

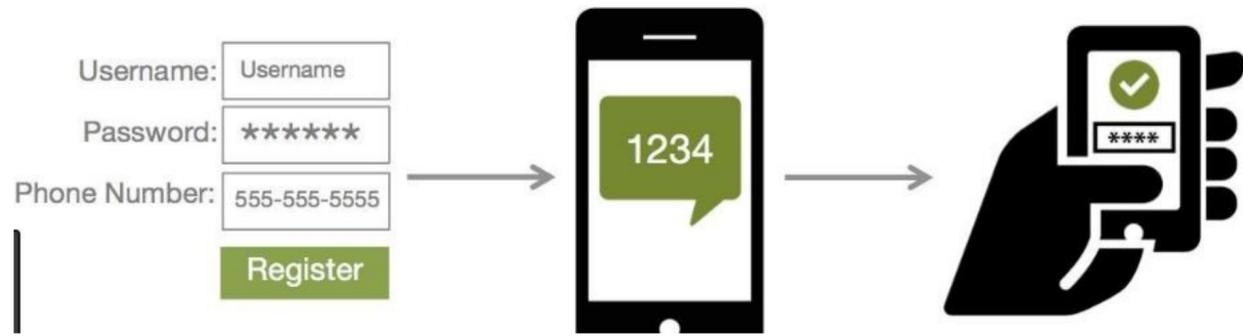


Pentera

Cymulate



СТОЙКОСТЬ ПАРОЛЕЙ



Аудит паролей корпоративной инфраструктуры, аудит подсистем усиленной аутентификации

S P E C O P S

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



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



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.



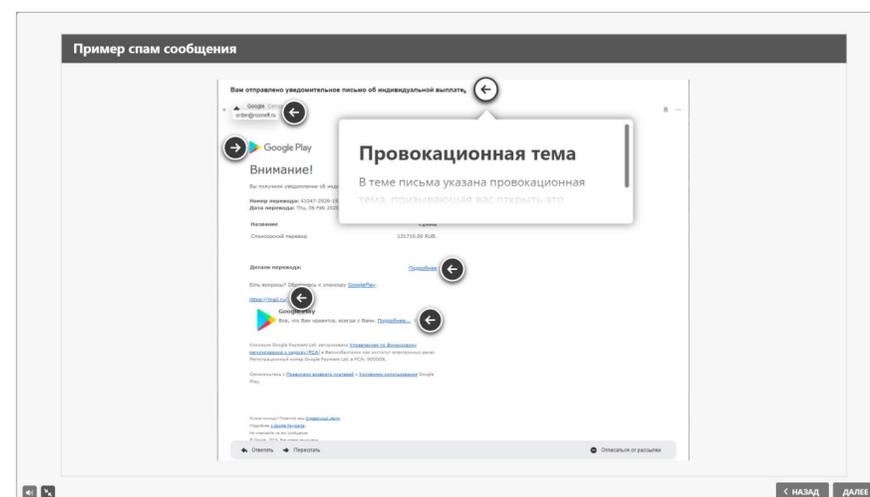
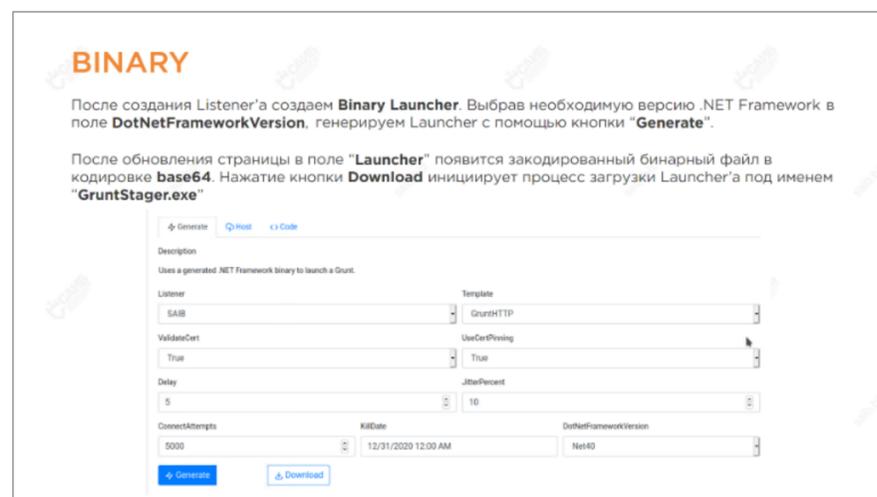
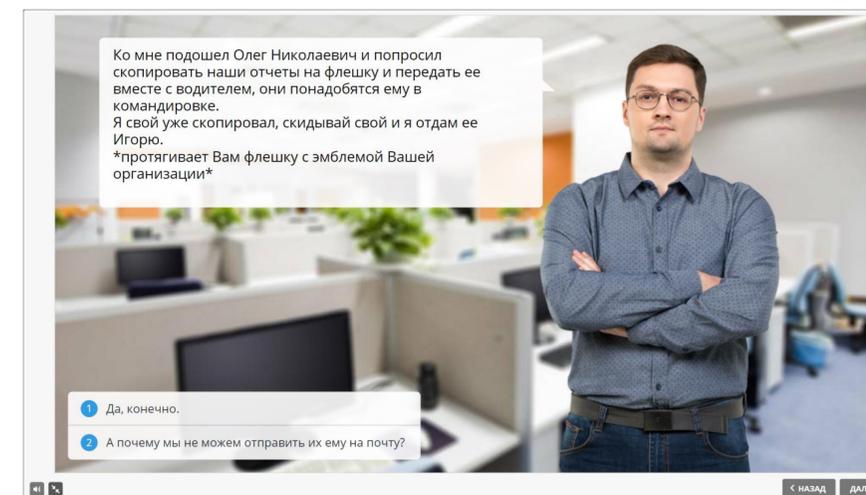
Обход системы безопасности

AV/EDR	Обфускация кода, использование тактик "Living off the Land"
Sandbox	Детектирование виртуализации, установленного ПО для мониторинга, анализ эмуляции работы пользователя
Шлюз безопасности и 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?



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



АНАЛИЗ ВЕБ-АКТИВНОСТИ ПОЛЬЗОВАТЕЛЕЙ

Имя	Зачислено	Действительность	Статус	Заголовок	Ссылка
080114	080228	000112	Ссылка	Делуру - имя на сайте. Автоподборный портал России	https://www.dellur.ru/
081928	081143	000115	Ссылка	Делуру - имя на сайте. Автоподборный портал России	https://www.dellur.ru/
081143	081315	000122	Ссылка		https://www.dellur.ru/
081235	082104	000128	Ссылка		https://www.dellur.ru/
082284	082318	000114	Ссылка	Делуру - имя на сайте. Автоподборный портал России	https://www.dellur.ru/
082318	082329	000111	Ссылка		https://www.dellur.ru/
082329	082402	000123	Ссылка	мысли не отключайте уведомление об уведомлении - Поиск в Google	https://www.dellur.ru/
082402	082420	000118	Ссылка	отправить уведомление об уведомлении по соглашению сторон - Поиск в Google	https://www.dellur.ru/
082420	082423	000120	Ссылка	Успешное по соглашению сторон. Проблемные моменты (рубли)	https://www.dellur.ru/
082423	082526	000120	Ссылка	Успешное по соглашению сторон. Проблемные моменты (рубли)	https://www.dellur.ru/
082526	083034	000108	Ссылка		https://www.dellur.ru/
083034	083050	000116	Ссылка		https://www.dellur.ru/
083050	083055	000120	Ссылка	Успешное по соглашению сторон. Проблемные моменты (рубли)	https://www.dellur.ru/
083055	083108	000112	Ссылка		https://www.dellur.ru/
083108	083111	000105	Ссылка		https://www.dellur.ru/
083111	083119	000106	Ссылка	из РФ уведомление - Поиск в Google	https://www.dellur.ru/
083119	083131	000112	Ссылка	TK РФ Статья 80. Распространение порнографических материалов и иных материалов, запрещенных к распространению	https://www.dellur.ru/
083131	083136	000105	Ссылка	из РФ уведомление - Поиск в Google	https://www.dellur.ru/
083136	083145	000109	Ссылка	уведомление расчет - Поиск в Google	https://www.dellur.ru/
083145	083321	000148	Ссылка	Расчет валют при уведомлении - Центр Зарплаты - СБС Центр	https://www.dellur.ru/
083321	083420	000149	Ссылка	Расчет при уведомлении в 2019 году	https://www.dellur.ru/
083420	083432	000123	Ссылка	Уведомление по собственному желанию - Консультант Плюс	https://www.dellur.ru/
083432	083431	000121	Ссылка	Уведомление по собственному желанию - Консультант Плюс	https://www.dellur.ru/
083511	083519	000108	Ссылка	уведомление расчет - Поиск в Google	https://www.dellur.ru/
083519	083523	000104	Ссылка	уведомление расчет - Поиск в Google	https://www.dellur.ru/

НАШИ КОМПЕТЕНЦИИ

Более 700
реализованных
проектов

Более 30
успешных
проектов с
компаниями
списка РБК
ТОП-500

20
специалистов
направления

Опыт
комплексных
проектов под
ключ

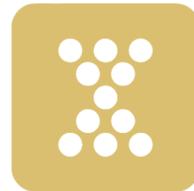
В наличии необходимые и сопутствующие лицензии



НАШИ КЛИЕНТЫ



ИТУРУП БАНК



ПримСоцБанк



Спасибо за внимание

ВАШИ ВОПРОСЫ



SKYPE: MAKSIM_PROKOPOV

EMAIL: PMD@AXXTEL.RU

Презентацию можно получить по запросу на info@axxtel.ru