Киберполигон Ampire

Российская платформа для тренировки специалистов по обеспечению информационной безопасности

Атакуют, обязательно атакуют

Хулиганы

Криминал

Наёмники

Кибервойска

Проактивная позиция

Не можем повлиять

1) Сам факт атаки
2) Квалификация атакующего
3) Инструментарий
4) Объём ресурсов

Можем повлиять

1) Стоимость атаки
2) Скорость реакции
3) Содержание реакции
4) Собственный опыт
5) Планы и изменения

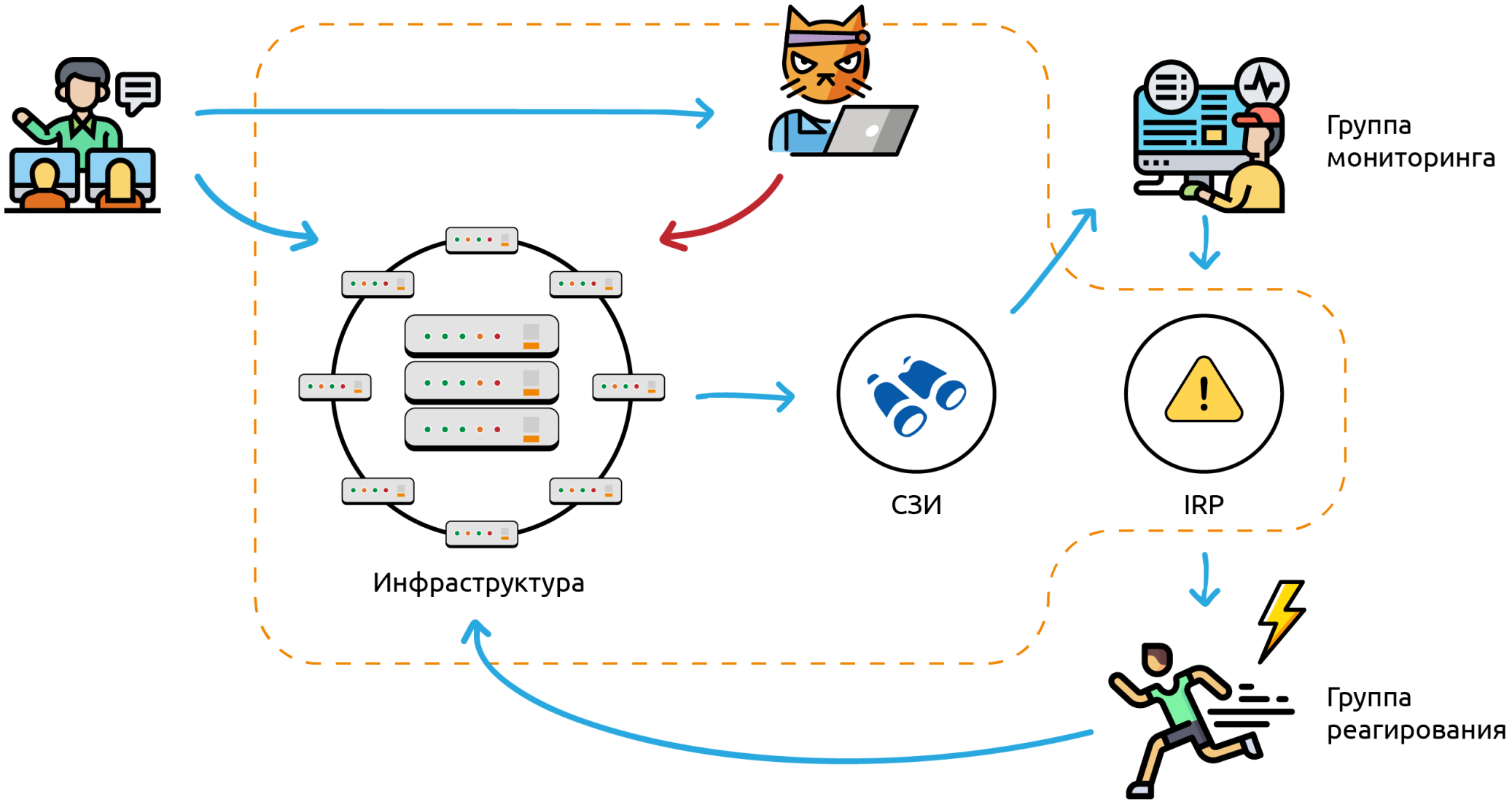
Способность действовать в экстренной ситуации зависит не от уровня знаний, а от уровня подготовки

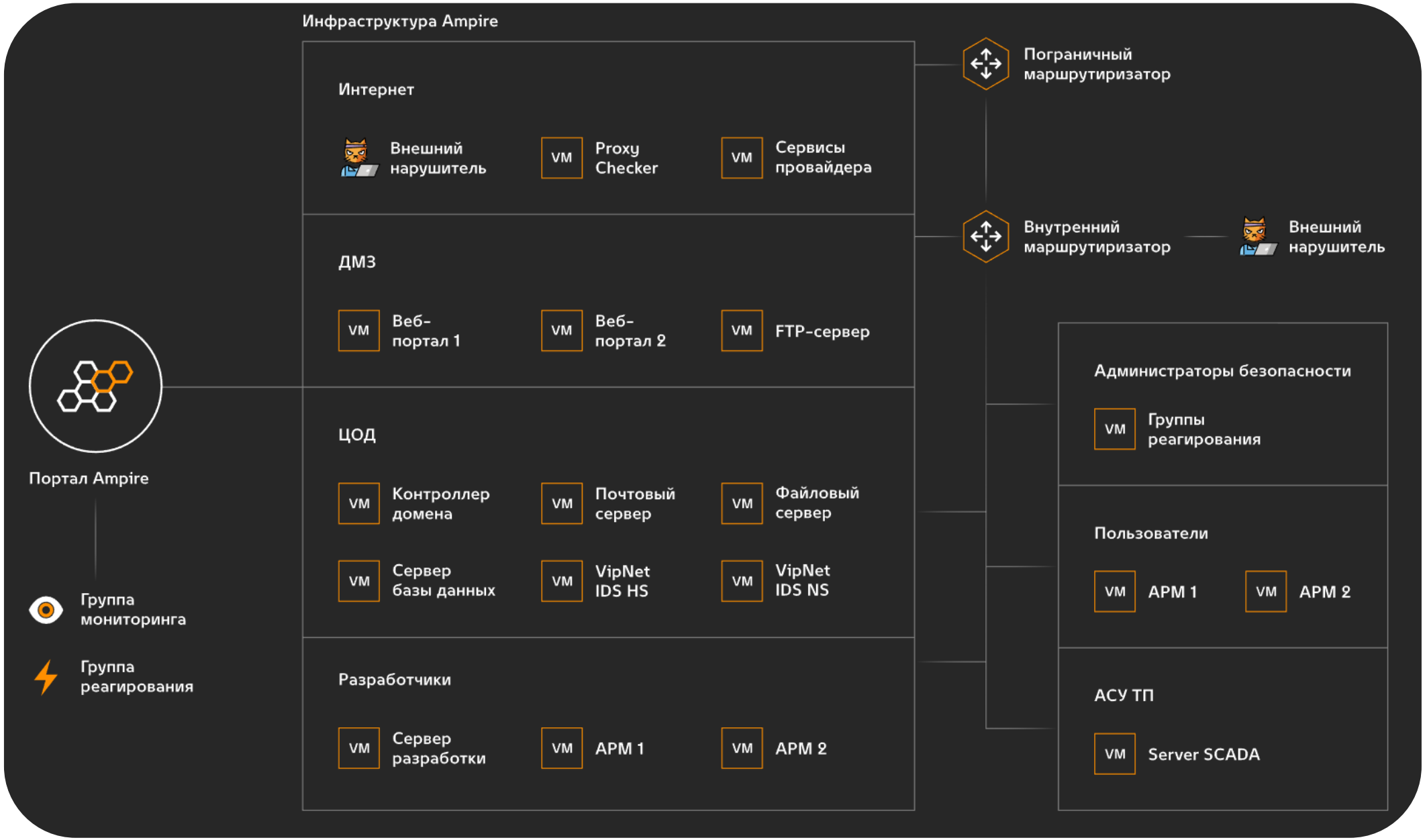
Целевая аудитория

- Школьники и студенты с базовым знанием TCP/IP сетей, которые планируют работать в сфере защиты информации.
- ИБ-специалисты, которые хотели бы выделиться среди других кандидатов глубокими знаниями в определённых областях.
- ИТ-специалисты: новички и те, кто хотел бы увеличить перечень навыков в резюме.

AMPIRE

Наша учебно-тренировочная платформа содержит сценарии различной сложности для проведения киберучений, сертификационных тестов и отработки необходимых навыков.


Группа
мониторинга
СЗИ
IRP
Инфраструктура
Группа
реагирования


Инфраструктура Ampire
Интернет
Внешний нарушитель
VM
Proxy Checker
VM
Сервисы провайдера
ДМЗ
VM
Веб-портал 1
VM
Веб-портал 2
VM
FTP-сервер
ЦОД
VM
Контроллер домена
VM
Почтовый сервер
VM
Файловый сервер
VM
Сервер базы данных
VM
VipNet IDS HS
VM
VipNet IDS NS
Разработчики
VM
Сервер разработки
VM
АРМ 1
VM
АРМ 2
Пограничный маршрутизатор
Внутренний маршрутизатор
Внешний нарушитель
Администраторы безопасности
VM
Группы реагирования
Пользователи
VM
АРМ 1
VM
АРМ 2
АСУ ТП
VM
Server SCADA
Портал Ampire
Группа мониторинга
Группа реагирования

Базовые сценарии киберучений

Защита базы данных предприятия

Защита контроллера домена предприятия

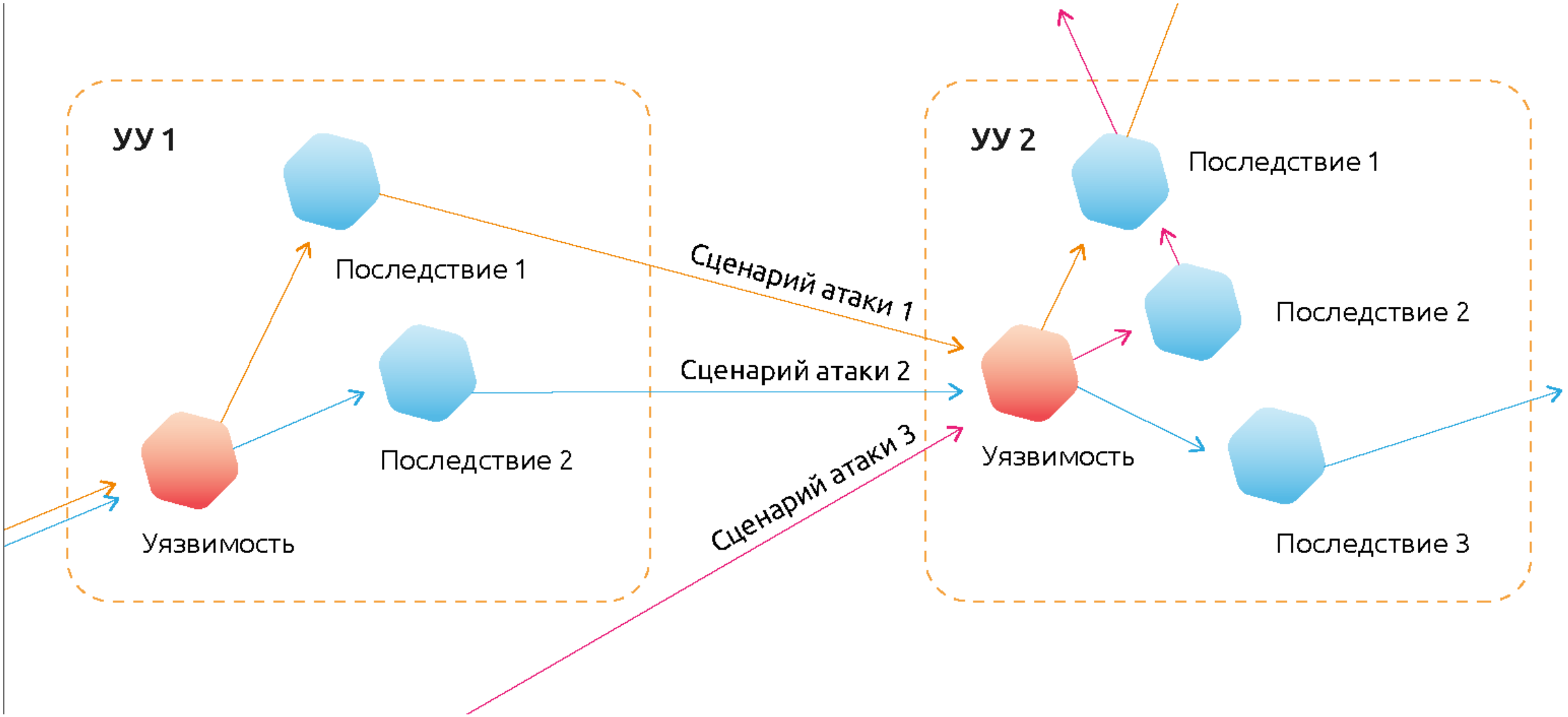
Защита файлового сервера предприятия (MS17-010)

Защита данных сегмента АСУ ТП

Защита научно-технической информации предприятия

Защита корпоративного портала от внутреннего нарушителя

Конфигуратор



СЗИ

ViPNet IDS NS

ViPNet IDS HS

ViPNet TIAS

IDS/IPS Snort

IDS/IPS Suricata

ELK

Security Onion

И почти любые другие

Типы проводимых занятий

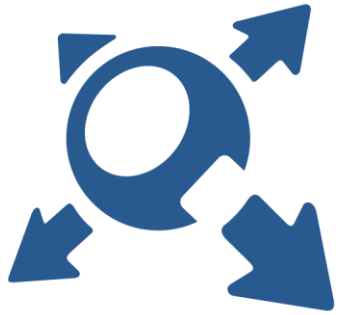
- Киберучения
- Анализ защищённости и аудит ИТ-инфраструктуры виртуальной организации
- Противодействие группе реальных нарушителей (концепция Red Team и Blue Team)
- Лабораторные работы по настройке средств безопасности и прикладных сервисов
- Киберквесты

Готовый класс

Навыки после прохождения курса

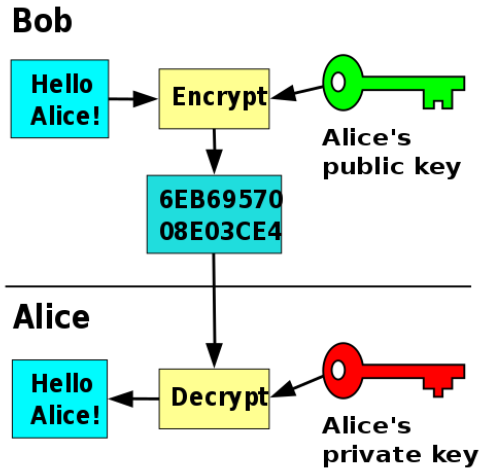
- Основные меры защиты сети, их преимущества и недостатки.
- Практика работы со средствами обнаружения вторжений (просмотр и фильтрация событий, правила выявления и реагирования на критичные события).
- Основные уязвимости веб-приложений и способы эксплуатации.






Навыки после прохождения курса

- Практика защиты веб-ресурсов при помощи WAF и исправления уязвимостей.
- Основные типы угроз для ОС и навыки защиты ОС.
- Средства защиты конечных точек.
- Навыки защиты технологический сетей.



Ключевые преимущества Ampire

- Полная независимость пользователя в проведении киберучений.
- Практические занятия для ИБ- и ИТ-специалистов любого уровня подготовки на «**двойнике**» реальной инфраструктуры.
- Полностью **автоматические сценарии атак**, разработанные экспертами по пентестам и базирующиеся на реальных инцидентах.
- Возможность создавать собственные сценарии по различным видам атак для ИТ-, ИБ-служб, операторов АСУТП, офиса, руководства.
- Подтверждение компетенций и развитие навыков группы реагирования на компьютерные атаки.
- ИТ-инфраструктура, СЗИ — всё вместе на одной платформе!

Спасибо за внимание!

Сергей Нейгер

Директор по развитию бизнеса компании «Перспективный мониторинг»

Sergey.Neyger@amonitoring.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363