ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Киберполигон Ampire

Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак

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

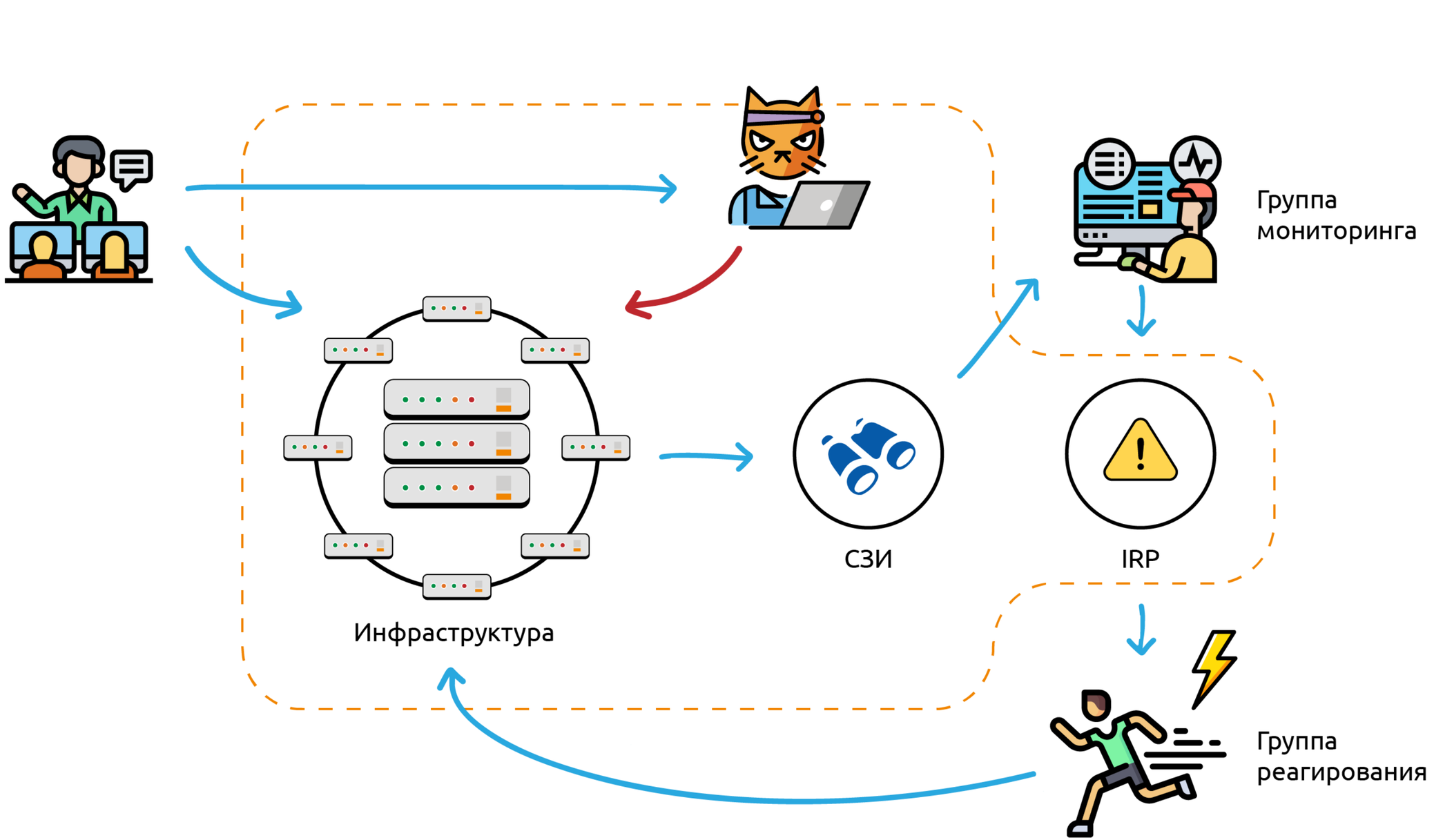
Способность действовать в экстренной ситуации зависит не от уровня знаний, а от уровня подготовки.

Целевая аудитория

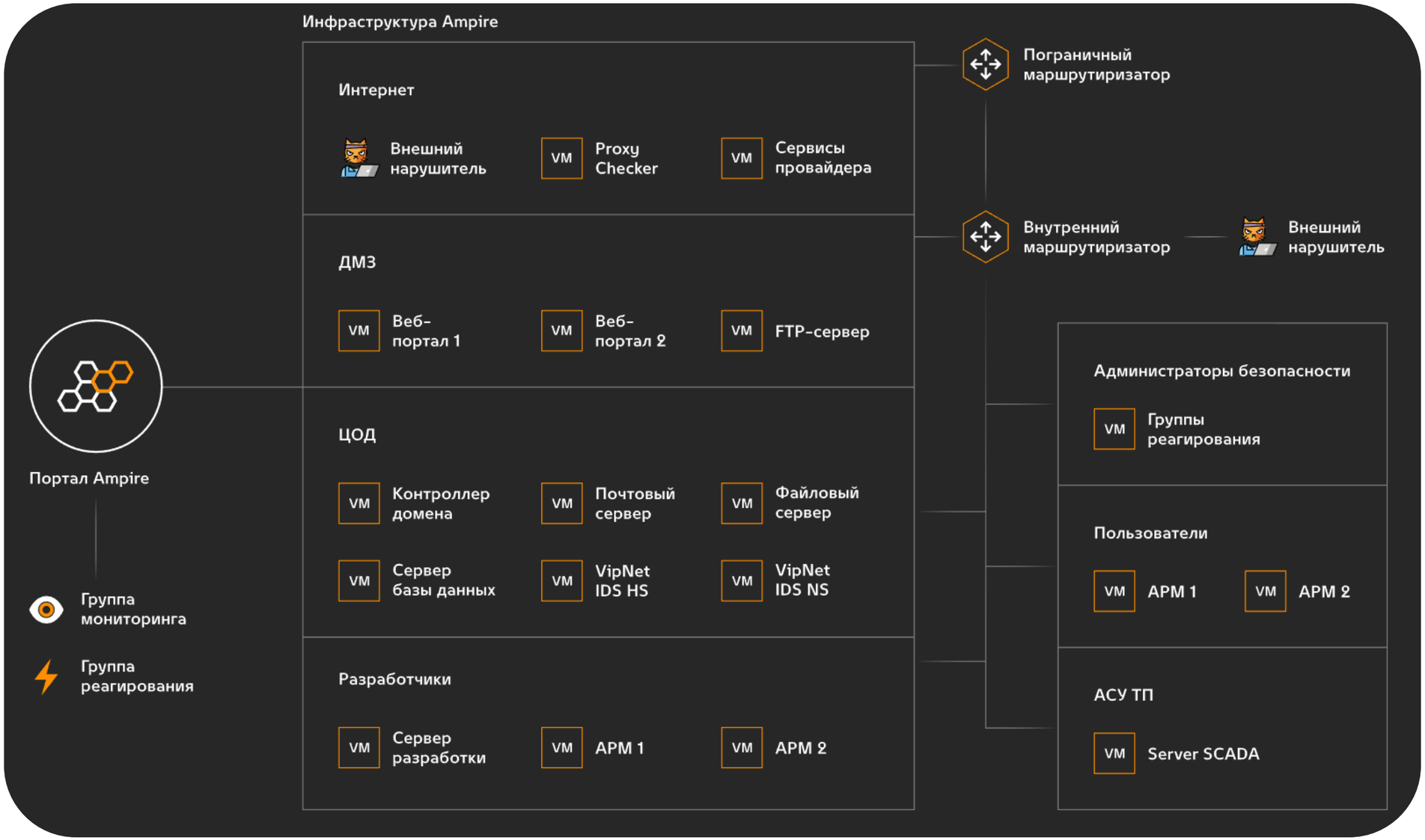
- Школьники и студенты с базовым знанием TCP/IP сетей, которые планируют работать в сфере защиты информации.
- ИБ-специалисты, которые хотели бы выделиться среди других кандидатов глубокими знаниями в определённых областях.
- ИТ-специалисты: новички и те, кто хотел бы увеличить перечень навыков в резюме.

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

Шаблон «Предприятие»



СЗИ

- VipNet IDS NS
- VipNet IDS HS
- VipNet TIAS
- IDS/IPS Suricata
- ELK
- Security Onion
- IDS/IPS Snort

И почти любые другие

Базовые сценарии киберучений

1. Защита базы данных предприятия
2. Защита контроллера домена предприятия
3. Защиты файлового сервера предприятия (MS17-070)
4. Защита данных сегмента АСУ ТП
5. Защита научно-технической информации предприятия
6. Защита корпоративного портала от внутреннего нарушителя

Типы проводимых занятий

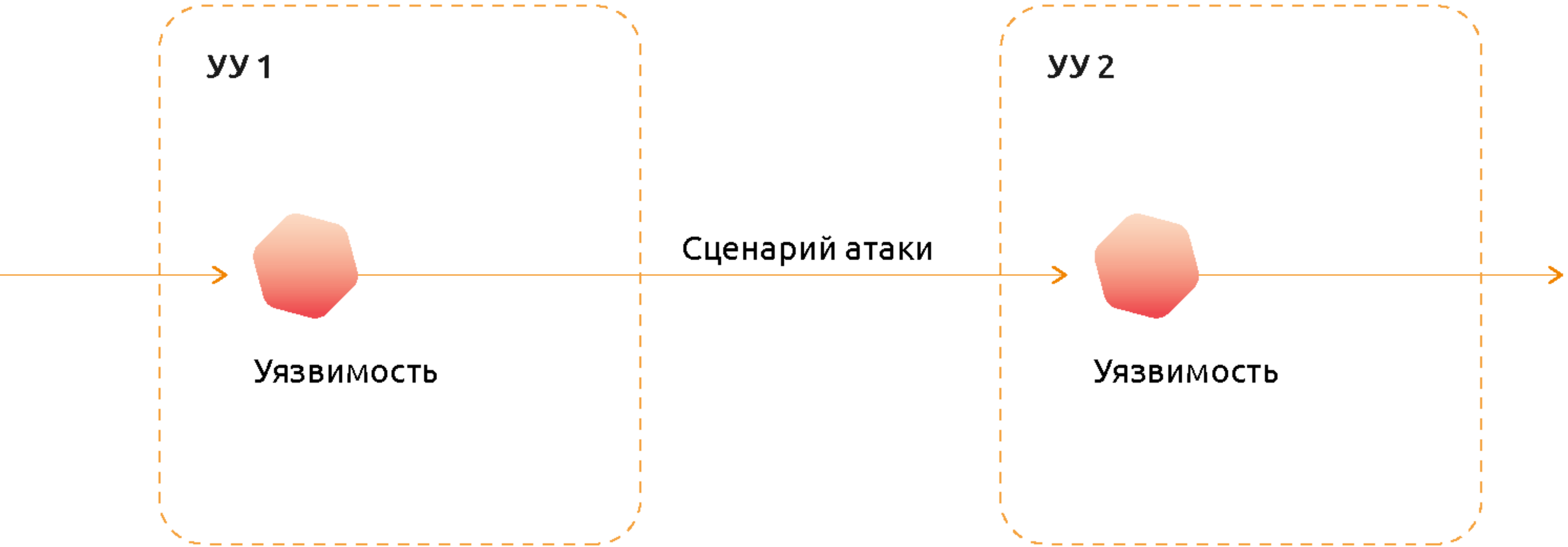
1. Киберучения
2. Анализ защищённости и аудит ИТ-инфраструктуры виртуальной организации
3. Противодействие группе реальных нарушителей (концепция Red Team и Blue team)
4. Лабораторные работы по настройке средств безопасности и прикладных сервисов
5. Киберквесты

Портал Ampire

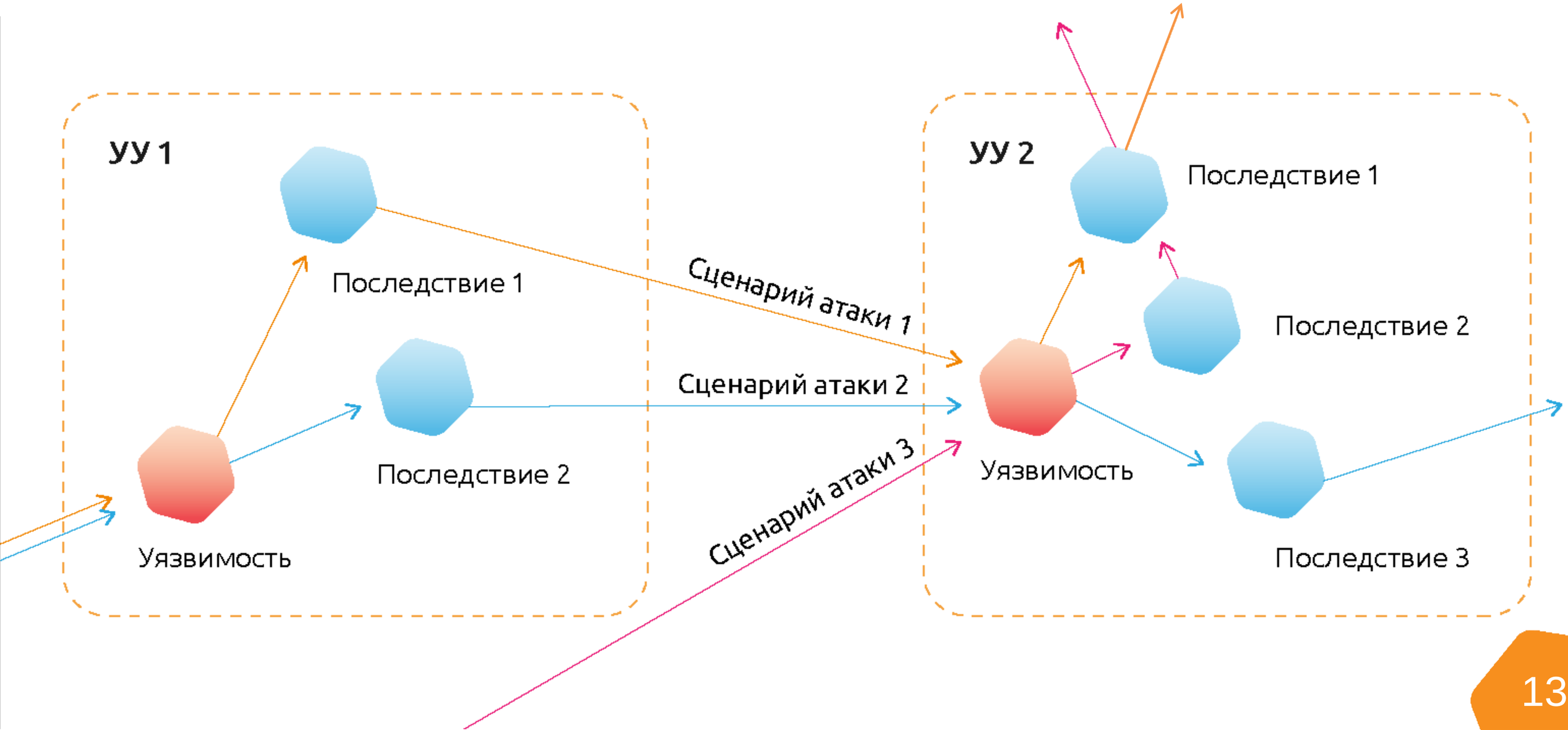
- Раздел преподавателя
- Раздел обучаемого
- Подключение к инфраструктуре тренировки
- Система управления инцидентами
- Мультиязычность
- Генератор отчётов

Идея Конфигуратора —
дать возможность преподавателю
самостоятельно подготавливать шаблон
организации и формировать вектор атаки

Было



Стало


УУ 1
Последствие 1
Последствие 2
Уязвимость
Сценарий атаки 1
Сценарий атаки 2
Сценарий атаки 3
УУ 2
Последствие 1
Последствие 2
Уязвимость
Последствие 3

Сотрудничаем с ВУЗами

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!

Правовые основания

1. Указ Президента РФ №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
2. Федеральный закон «О безопасности критической информационной инфраструктуры» 187-ФЗ.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» 149-ФЗ.
4. Концепция ГосСОПКА.

Оснащение лабораторий

Лаборатория на основе Учебно-тренировочной платформы Ampire практически полностью выполняет требования федеральных государственных стандартов к материально-техническому и учебно-методическому обеспечению программ по специальностям в информационной безопасности и позволяет региону в короткие сроки подготовить специалистов, обладающих практическими навыками выявления компьютерных атак, расследования инцидентов информационной безопасности, реализации защитных мер для нейтрализации существующих недостатков безопасности в информационных сетях общего и специального назначения (связь, энергетика, финансовая сфера, ТЭК, промышленные предприятия различных отраслей).

Организационные преимущества

1. Круглосуточная готовность проводить занятия. Старт тренировки через 2 минуты после начала занятия.
2. Возможность зарабатывать на ДПО и повышении квалификации.
3. Бессрочная лицензия. Продолжит работать даже по истечению срока оплаченной технической поддержки.
4. Возможность заказной разработки тренировочной ИТ-инфраструктуры и сценариев.

Техническая зрелость

1

Возможно удалённое подключение к платформе

2

Устанавливается непосредственно на инфраструктуре заказчика

3

Единственная учебно-тренировочная платформа, в состав которой входят СЗИ линейки ViPNet

В поставку входят

- Программное обеспечение Ampire
- Подготовка преподавателей для работы с комплексом
- Рабочая программа, методические материалы
- Техническая поддержка
- Обновление контента

Комплекс продолжит работать и без техподдержки

Требования к площадке

- Высшие учебные заведения и учебные центры могут разместить киберполигон Ampire в любой стандартной аудитории.

- Минимальный размер класса, достаточный для проведения тренировки для 8–10 человек — ок. 35–40 м².

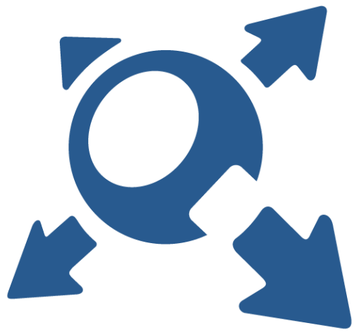
- Оборудование киберполигона могут поддерживать уже существующие ИТ-службы учебных заведений.

Пример готового класса

Навыки после прохождения курса

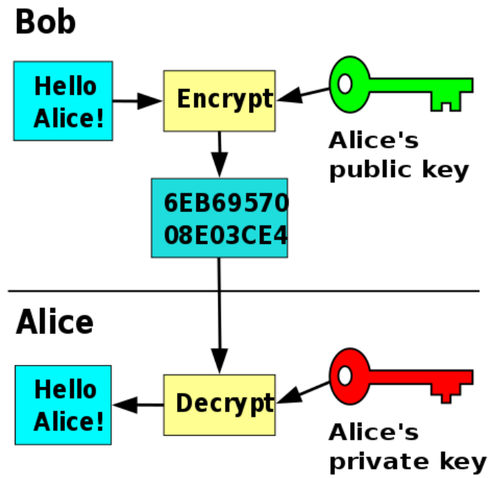
- Основные меры защиты сети, их преимущества и недостатки.
- Практика работы со средствами обнаружения вторжений (просмотр и фильтрация событий, правила выявления и реагирования на критичные события).
- Основные уязвимости веб-приложений и способы эксплуатации.






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.
- Криптографическая защита конфиденциальных данных при передаче и хранении.
- Навыки защиты технологических сетей.



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

t.me/pm_public

amonitoring.ru

Сергей Нейгер

Директор по развитию бизнеса
«Перспективный мониторинг»

+7 (999) 210-48-94

Sergey.Neyger@amonitoring.ru