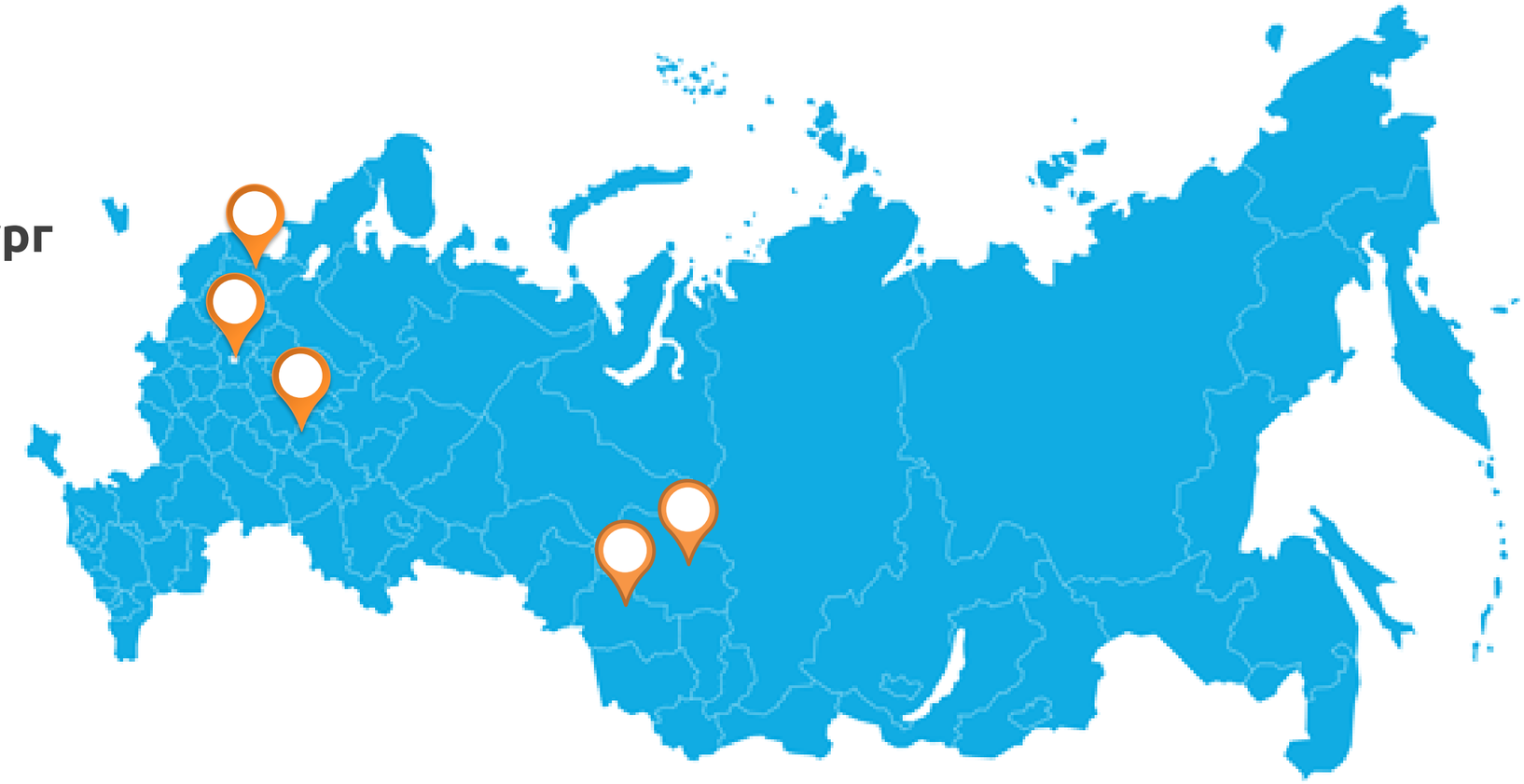
ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

infotecs®

Непрерывное взаимодействие с Центром ГосСОПКА

География офисов АО «ПМ»

Санкт- Петербург
Москва
Пенза
Новосибирск
Томск



Входим в группу компаний «ИнфоТеКС»

ПМ сегодня

12

Лет на рынке услуг SOC и исследования защищённости

5

Лет центр ГосСОПКА

>1600

Выполненных ИБ проектов

12

Действующих киберполигонов Ampire

300+

Проведенных киберучений

3000+

ИБ специалистов прошли обучение на Ampire

Центр мониторинга (в цифрах)

15 000
События в секунду

> 20 000
Конечных агентов

6
Поддерживаем SIEM/LC

> 400
Сетевых сенсоров IDS/IPS

> 50
Поддерживаем ViPNet TIAS

> 150 000
Инфраструктура узлов

2014
год запуска

с 2017 года
Центр ГосСОПКА класса А

24/7
режим сопровождения

Проекты в СФО

Кузбасс

1,2,3 линия

Красноярский край

2,3 линия

Омская область

1,2,3 линия

Республика Тыва

1,2 линия

Холдинг «Новапорт»

1,2,3 линия

Алтайский край

1,2 линия

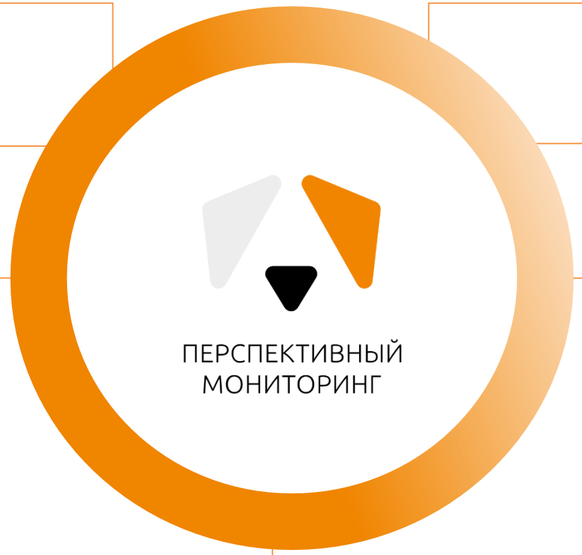
Направления деятельности

Исследование защищённости

- Пентест
- Аудит ИБ
- Оценка соответствия требованиям Банка России

SOC

- Коммерческий SOC
- Подключение к ГосСОПКА
- Расследование инцидентов ИБ



Продукты

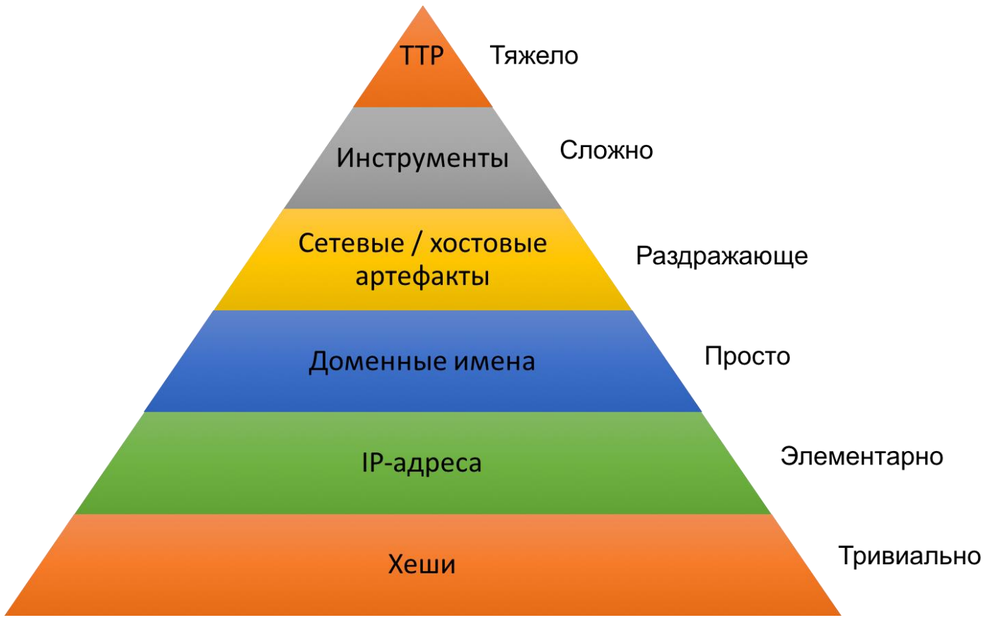
- Экспертные данные AMRules
- Киберполигон Ampire

Сквозная экспертиза по всем направлениям деятельности ПМ

Экспертные данные
TI АО «ПМ»

1. т.н. «Базы решающих правил» (БРП, включают наборы snort, yara, ossec, suricata правила)
2. TI feeds (IoC в STIX или любом другом пользовательском формате)
3. AM Rules (Свидетельство Роспатента №2016620316 от 03.03.2016 г.)
4. Бюллетени ИБ

Индикаторы компрометации (IoC)



Пирамида индикаторов компрометации в зависимости от сложности получения данных (т.н. «Пирамида боли» David J Bianco)

*https://www.securitylab.ru/blog/personal/Business_without_danger/320988.php

IPv4 Domain Хэши (MD5, SHA1)

URL Транзакционные (MTA, User-agent) Имена файлов/путь

mutex Значения реестра e-mails

Наиболее популярные типы индикаторов компрометации

Разведка	Оснащение	Доставка	Заражение	Инсталляция	Получение управления	Выполнение действий
Файл – имя Файл URI – URL HTTP - GET HTTP – User Agent URI – имя домена Адрес – e-mail Адрес – IPv4	Файл – путь Файл URI – URL	Поведение Файл – имя Файл – путь Файл URI – URL HTTP – POST Заголовок e-mail – Тема Заголовок e-mail – X-Mailer URI – имя домена Хеш – MD5 Хеш – SHA1 Адрес – e-mail Адрес – IPv4	Поведение Ключ реестра Win Файл – имя Файл URI – URL URI – имя домена Хеш – MD5 Хеш – SHA1 Адрес – CIDR Адрес – IPv4	Код – Бинарный код Процессы Win Ключ реестра Win Файл – имя Файл – путь Файл URI – URL HTTP – GET HTTP – User Agent URI – имя домена Хеш – MD5 Хеш – SHA1 Адрес – e-mail Адрес – IPv4	Поведение Процессы Win Ключ реестра Win Файл URI – URL HTTP – GET HTTP – POST HTTP – User Agent URI – имя домена Хеш – MD5 Адрес – e-mail Адрес – IPv4	Поведение Процессы Win Сервисы Win Файл – Путь Файл – Имя Файл URI – URL URI – имя домена Хеш – MD5 Хеш – SHA1 Адрес – IPv4

Наложение известных индикаторов компрометации на этапы Kill Chain

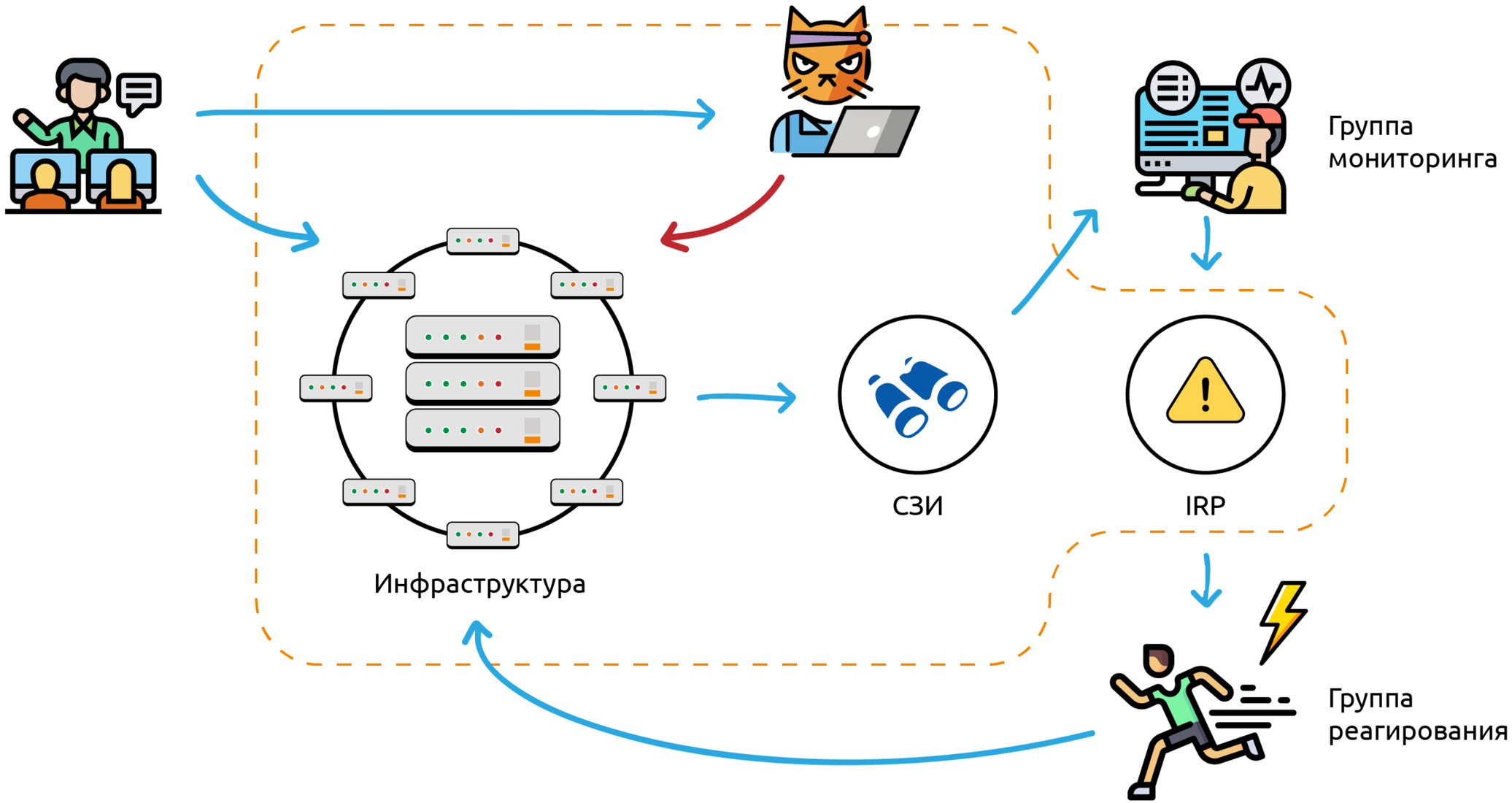
Какие проблемы решает Центр ГосСОПКА?

Что входит

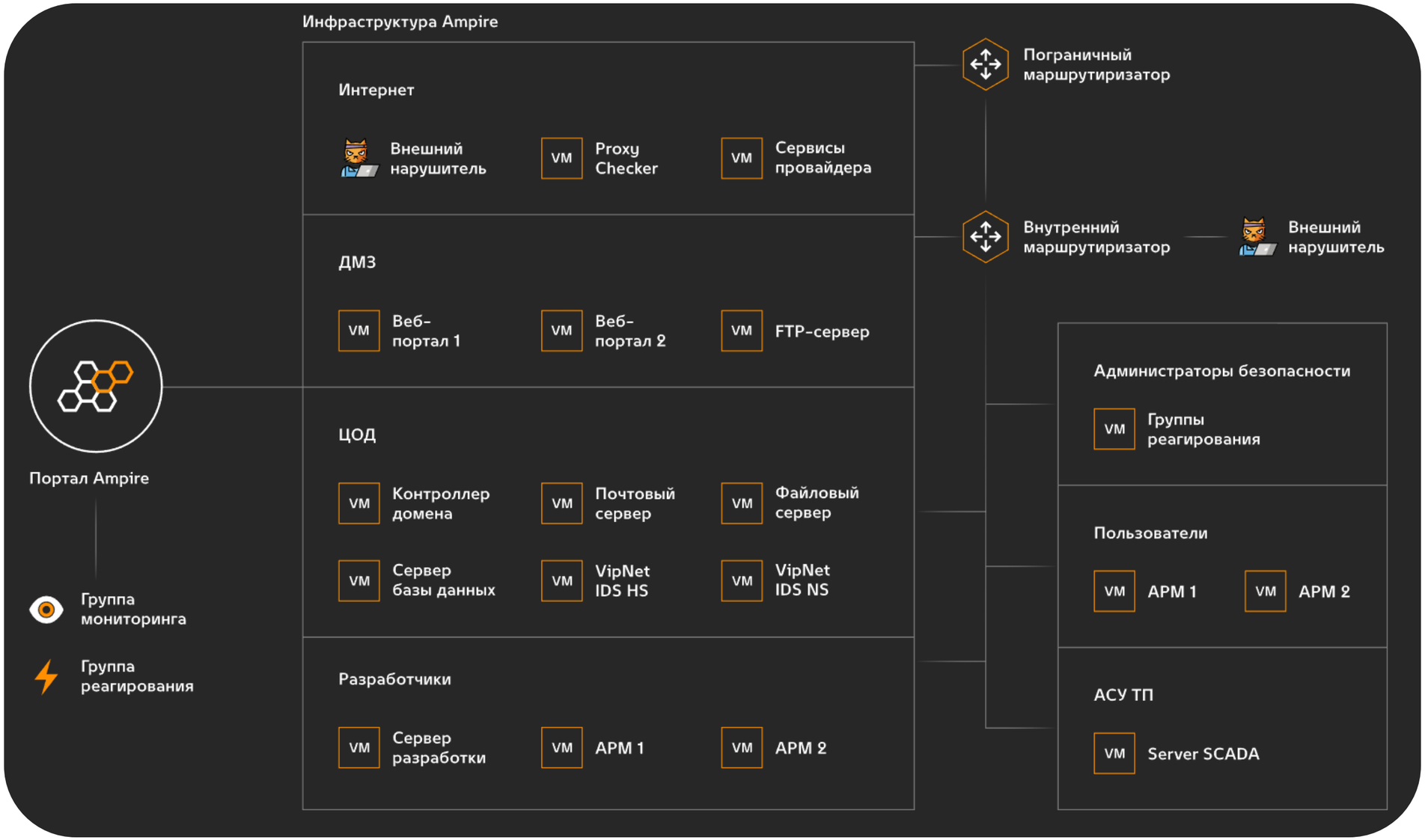
1) Анализ компьютерных атак (инцидентов)
2) Единая Система управления инцидентами
3) Тесты на проникновение (Pentest)
4) Тюнинг конфигурации WAF/SIEM
5) Взаимодействие с НКЦКИ, ФСО России
6) TI Feeds (IOC)
7) Эксперты-исследователи. База знаний
8) Процессы. SLA. Playbook/runbook
9) Категорирование объектов КИИ
10) **Киберполигон Ampire**

И многое другое

Киберполигон


Группа
мониторинга
СЗИ
IRP
Инфраструктура
Группа
реагирования

Шаблон «Предприятие»



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

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.

Сотрудничаем с ВУЗами

МТУСИ
Московский технический университет связи и информатики

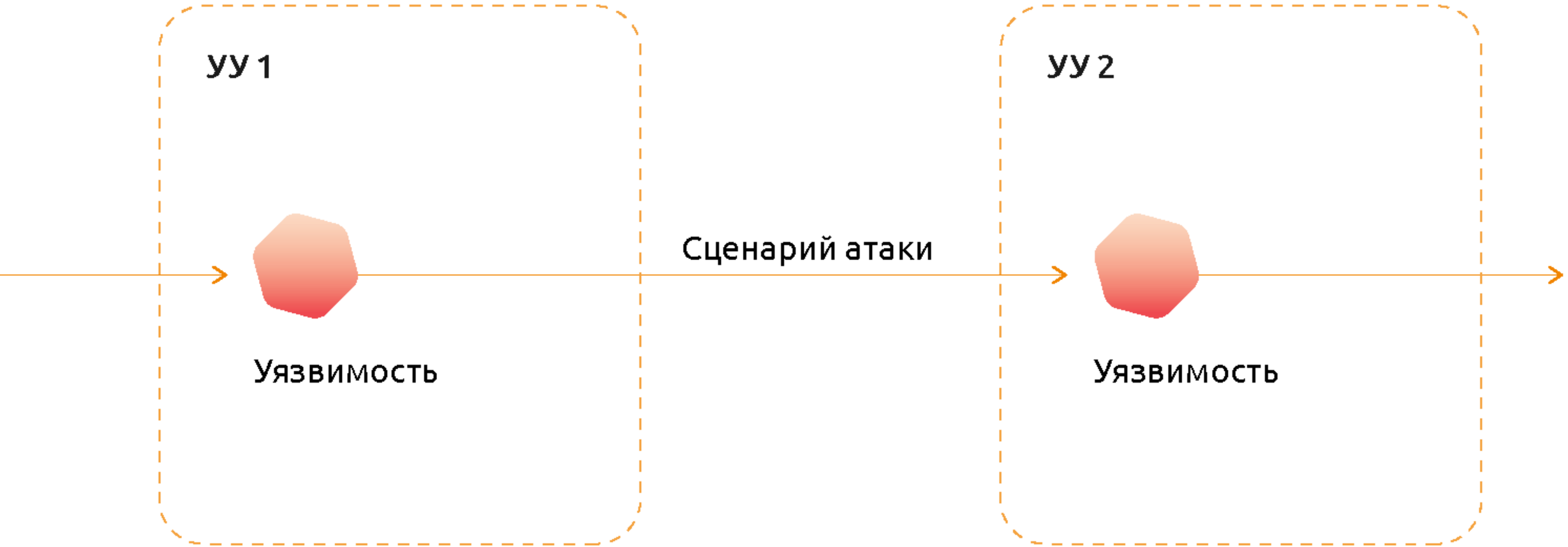
1890
КНИТУ

МИРЭА
Российский технологический университет

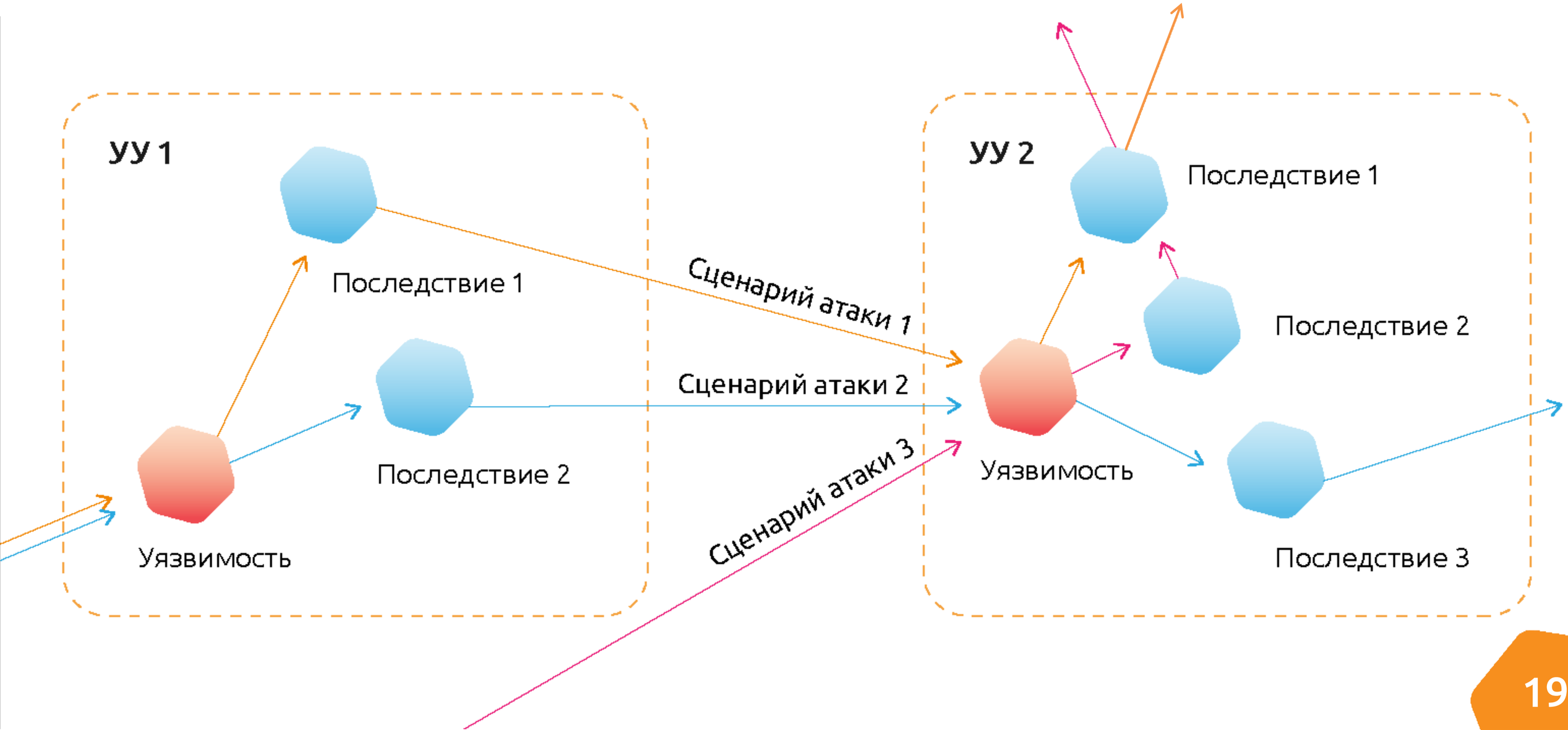
ТУСУР | TUSUR UNIVERSITY

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

Карточка тренировки

AMPIRE

Квест 29_11

ОБЩАЯ ИНФОРМАЦИЯ | ИНЦИДЕНТЫ | УЧАСТНИКИ | СХЕМА ШАБЛОНА | ЛОГИ СОБЫТИЙ АТАКИ

ОБЩАЯ ИНФОРМАЦИЯ О ТРЕНИРОВКЕ

Название тренировки	Квест 29_11
Шаблон	Предприятие (конфигуратор)
Сценарий	Защита SCADA
Группа	test
Статус тренировки	завершена
Доступные действия	скачать отчёт

Начало тренировки 29.11.2022 12:16
Конец тренировки 29.11.2022 13:11

ПРОГРЕСС АТАКИ 100%

Схема шаблона

Скачать методические материалы

Участники

ГРУППА test

МОНИТОРИНГ	в сети	0 / 1
РЕАГИРОВАНИЕ	в сети	0 / 2
ЛИДЕР РЕАГИРОВАНИЯ	не в сети	

3/3

WORDPRESS DUPLICATOR — УСТРАНЕНО

ZEROLOGON — УСТРАНЕНО

IGSS32 — УСТРАНЕНО

ИНЦИДЕНТЫ

Новые	0/0
Рассматриваются	0/0
Закрытые	0/0
Цепочки кибератаки	0/1

3/3

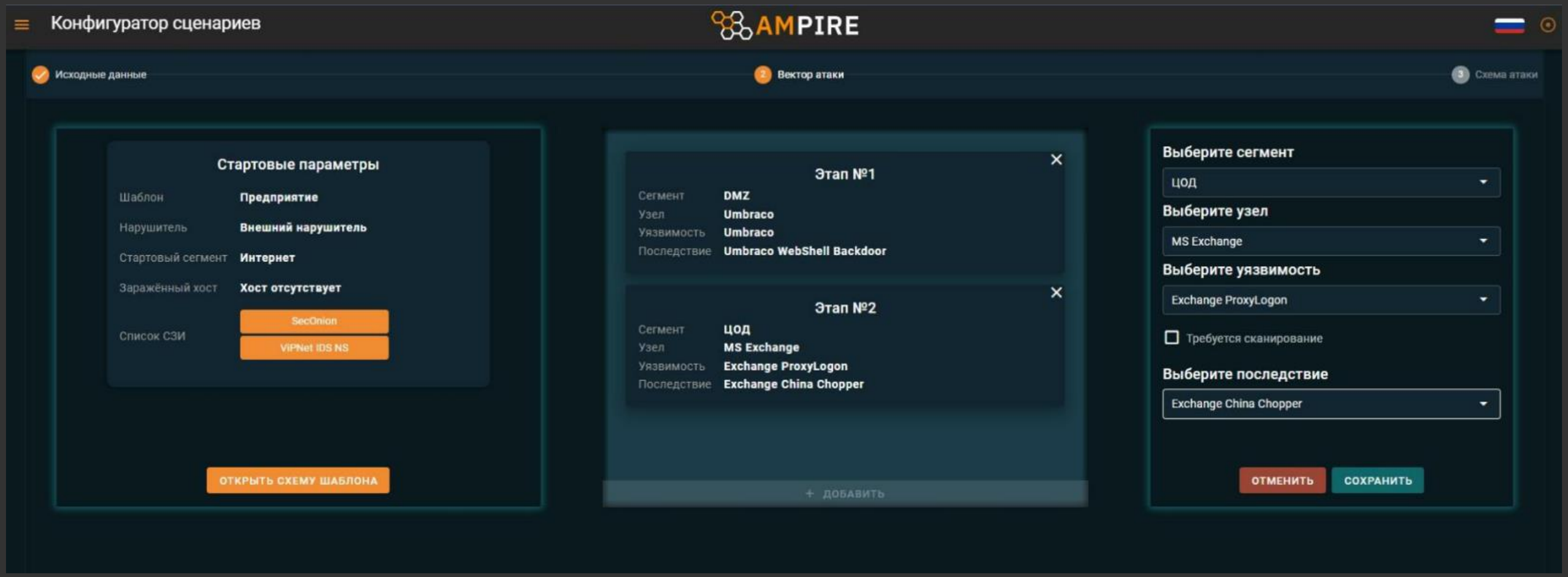
IGSS32 REVERSE SHELL — УСТРАНЕНО

AD USER — УСТРАНЕНО

WORDPRESS DEFACE — УСТРАНЕНО

ДОСТУПНЫЕ РЕСУРСЫ

Удалённое рабочее место	10.10.211.235
SecOnion	10.10.211.114
ViPNet TIAS	Информация отсутствует
ViPNet IDS NS	10.10.211.128


Конфигуратор сценариев
AMPIRE
Исходные данные
2 Вектор атаки
3 Схема атаки
Стартовые параметры
Шаблон Предприятие
Нарушитель Внешний нарушитель
Стартовый сегмент Интернет
Заражённый хост Хост отсутствует
Список СЗИ
SecOnion
ViPNet IDS NS
ОТКРЫТЬ СХЕМУ ШАБЛОНА
Этап №1
Сегмент DMZ
Узел Umbraco
Уязвимость Umbraco
Последствие Umbraco WebShell Backdoor
Этап №2
Сегмент ЦОД
Узел MS Exchange
Уязвимость Exchange ProxyLogon
Последствие Exchange China Chopper
+ ДОБАВИТЬ
Выберите сегмент
ЦОД
Выберите узел
MS Exchange
Выберите уязвимость
Exchange ProxyLogon
Требуется сканирование
Выберите последствие
Exchange China Chopper
ОТМЕНИТЬ
СОХРАНИТЬ

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

Целевая аудитория

- **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 Junior —

специальная версия учебно-тренировочной платформы Ampire для проведения занятий в области кибербезопасности и кибергигиены для школьников

IT – киберсреда и информационная безопасность

Дополнительная общеобразовательная общеразвивающая программа «IT-КИБ» является авторской и относится к программам технической направленности.

Цель – формировать у обучающихся мышление, направленное на понимание и использование цифровых, информационных и коммуникационных технологий посредством кейсовой системы обучения и проектно-исследовательской деятельности

Задачи обучения

- сформировать навыки работы с информацией
- формировать предметные компетенции по защите информации и информационной безопасности, веб-технологиями
- освоить терминологию в области IT - технологий
- владение лексикой технического английского в области IT-индустрии
- Формирования мировоззрения человека информационного общества и культуры как совокупности знаний, умений и навыков, необходимых в условиях развития цифровой экономики
- избирательно относиться к информации в окружающем информационном пространстве

Задачи развития

- стимулировать интерес к техническим наукам и информационным технологиям
- стимулировать познавательную и творческую активность обучающихся посредством включения их в различные виды соревновательной и публичной деятельности
- выявлять и развивать soft skills (гибкие навыки), которые помогают решать жизненные задачи
- развивать память, внимание, логическое, пространственное и аналитическое мышление, креативность и лидерство
- развивать способности исследовательской и проектной деятельности

Задачи воспитания

- развивать умение командной работы, координацию действий
- воспитывать ценностное отношение к информации, продуктам интеллектуальной деятельности (своей, чужой, командной)
- подготовить осознанный выбор дальнейшей траектории обучения в рамках раннего профориентирования
- соблюдать нормы информационной культуры, этики и права
- расширять кругозор и культуру, межкультурную коммуникацию
- организовать работу малого коллектива исполнителей в профессиональной деятельности, создание своего Центра управления безопасностью
- выявлять и повышать готовность к участию в соревнованиях разного уровня

Актуальность, новизна и значимость программы

1. воспитание нового А-поколения, отвечающего по своему уровню развития и образу жизни условиям цифрового общества

2. получат навыки по планированию и проведению исследований интернет-пространства, количественному и качественному анализу информации, выявлению и систематизации событий, информационных поводов

3. ускоренное техническое образование детей и реализацию научно-технического потенциала российской молодежи, привлечение внимания молодёжи к профессиям IT-сектора

Отличительные особенности программы

1) **Модульная и кейсовая система обучения, проектная деятельность обучаемого, освоение цифровых навыков.**

2) **Практические занятия на современной отечественной учебно-тренировочной платформе «Ampire», специально интегрированной под запросы.**

3) **Быстрый способ погрузиться в мир новой и востребованной профессии, это «Билет в будущее»**

4) **Реализованы лучшие мировые практики противодействия кибератакам, уникальные обучающие материалы и лабораторные работы:**

   - полноценный IT-ландшафт

Условия и сроки реализации программы

- Категория обучающихся: от 14 до 18 лет (7-11 классы).
- Наполняемость группы не менее 8 и не более 14 человек.
- Форма обучения – очная, очно-заочная с использованием дистанционных и ИКТ.
- К занятиям допускаются дети без специального отбора.
- Продолжительность учебного года – 36 недель.
- Форма занятий - групповая, по подгруппам, в парах или индивидуально.
- Объем учебной нагрузки в год – 144 часов (может варьироваться), в неделю – 4 часа.

Планируемые результаты

Обучающийся будет знать:

- принципы работы интернета вещей;
- угрозы в интернет-ресурсах и противодействовать им;
- базовые понятия защиты информации и информационной безопасности;
- о современном состоянии, тенденциях и перспективах развития в области систем мониторинга и регистрации событий ИБ;
- о системах обнаружения и предотвращения компьютерных атак;
- принципы действия, технологию использования и методику применения средств защиты информации.

Планируемые результаты

Обучающийся будет уметь:

- искать достоверную информации в интернете;
- искать информацию в различных источниках и структурировать ее;
- безопасно и рационально использовать личные и персональные данные;
- работать в команде;
- критически мыслить и объективно оценивать свои результаты;
- использовать современные отечественные СОВ;
- проводить мониторинг и анализ событий и инцидентов ИБ;
- работать в команде и публично демонстрировать свои проекты.

Отслеживания результатов освоения программы

- промежуточная аттестация по окончанию модуля
- контрольные задания по окончанию темы
- педагогическое наблюдение в ходе занятий
- психологическая диагностика
- командные зачеты
- отображения результатов в автоматически формируемых отчётах в «Ampire»
- участие в соревнованиях различного уровня

Программа курса минимум

№ раздела	Наименование раздела	Количество часов обучения			
		Всего	Лекции	ПЗ	СР
1	Эффективный поиск информации в интернете	7	1	6	
2	Безопасность в социальных сетях	7	1	6	
3	Социальная инженерия и методы защиты от нее	4	1	3	
Итого:		18	3	15	

Лабораторный практикум минимум

№ п/п	Наименование раздела	Способ реализации лабораторных работ	(час.)
Тема 1. Эффективный поиск информации в интернете			
1	Информационно-поисковые системы в интернете	Занятия проводятся на специально подготовленных виртуальных машинах Комплекса для каждого обучающегося	2
2	Методы эффективного поиска в сети интернет		2
3	Google-хакинг		2
Тема 2. Безопасность в социальных сетях			
4	Методы защиты от угроз в социальных сетях	Занятия проводятся на специально подготовленных виртуальных машинах Комплекса для каждого обучающегося на примере созданных профилей в соцсети ВКонтакте	3
5	Кибербуллинг и доксинг		3
Тема 3. Социальная инженерия и методы защиты от нее			
6	Фишинг и антифишинг	Занятия проводятся на специальном сценарии Комплекса, в котором демонстрируются примеры фишинга	2
7	Аудит паролей	Занятия проводятся на специальном сценарии Комплекса, в котором демонстрируются примеры атак на использование слабых паролей	1

Программа курса, распределение учебного времени по разделам

№ раздела	Наименование раздела	Количество часов обучения			
		Всего	Лекции	ПЗ	СР
1	Эффективный поиск информации в интернете	10	3	6	1
2	Безопасность в социальных сетях	12	4	8	
3	Социальная инженерия и методы защиты от нее	12	3	8	1
4	Управление инцидентами ИБ. Технологии обнаружения компьютерных атак	10	2	4	4
5	Обнаружение, анализ и расследование инцидентов ИБ	14	4	10	
6	Обнаружение, анализ и устранение последствий компьютерных атак на базе ПК «Ampire»	60	12	48	
7	Проектная деятельность	26	2	6	18
Итого:		144	30	90	24

Лабораторный практикум

№ п/п	Наименование раздела	Способ реализации лабораторных работ	(час.)
Тема 1. Эффективный поиск информации в интернете			
1	Информационно-поисковые системы в интернете	Занятия проводятся на специально подготовленных виртуальных машинах Комплекса для каждого обучающегося	2
2	Методы эффективного поиска в сети интернет		2
3	Google-хакинг		2
Тема 2. Безопасность в социальных сетях			
4	Методы защиты от угроз в социальных сетях	Занятия проводятся на специально подготовленных виртуальных машинах Комплекса для каждого обучающегося на примере созданных профилей в соцсети ВКонтакте	4
5	Кибербуллинг и доксинг		4
Тема 3. Социальная инженерия и методы защиты от нее			
6	Фишинг и антифишинг	Занятия проводятся на специальном сценарии Комплекса, в котором демонстрируются примеры фишинга	4
7	Аудит паролей	Занятия проводятся на специальном сценарии Комплекса, в котором демонстрируются примеры атак на использование слабых паролей	4

Лабораторный практикум

Тема 4. Управление инцидентами информационной безопасности. Технологии обнаружения компьютерных атак			
8	Обнаружение атак как механизм защиты	Занятия проводятся на модели ИТ-инфраструктуры офисной сети. Проводится ее изучение с элементами аудита	2
9	Уязвимости, угрозы и модели нарушителя		2
Тема 5. Обнаружение, анализ и расследование инцидентов информационной безопасности			
10	Средства обнаружения компьютерных атак	Занятия проводятся на модели ИТ-инфраструктуры офисной сети. Проводится ее изучение и работа со средствами обнаружения компьютерных атак	4
11	Сетевой сенсор системы обнаружения атак ViPNet IDS NS	Занятия проводятся на модели ИТ-инфраструктуры офисной сети. Проводится ее изучение и работа со средствами обнаружения компьютерных атак	2
12	Сетевые атаки (вторжения)		1
13	Поиск и анализ атак		3

Практические занятия

№ п/п	Наименование темы	Способ реализации практической части	час
Киберучения на базе Программного комплекса			
1	Описание основного процесса проведения киберучений. Ролевая модель	Знакомство с возможностями личного кабинета обучающегося	1
2	Защита базы данных предприятия	Занятия проводятся на упрощенных сценариях Комплекса, адаптированных для учащихся старших классов	4
3	Защита контроллера домена предприятия		4
4	Защита данных сегмента файлового сервера		4
5	Защита данных сегмента АСУ ТП		4
6	Защита научно-технической информации предприятия		4
7	Защита корпоративного портала от внутреннего нарушителя		4
8	Защита корпоративной информационной сети со сценариями различной сложности, созданных на конфигураторе		23

Содержание программы

№	Наименование раздела/темы	Содержание
Тема 1. Эффективный поиск информации в интернете		
1	Информационно-поисковые системы в интернете	Типы поисковых систем, принципы работы злоумышленников в поисковых системах
2	Методы эффективного поиска в сети интернет	Использование специальных операторов поиска
3	Google-хакинг	Методы защиты от злоумышленников при работе в поисковых сетях

Содержание программы

Тема 2. Безопасность в социальных сетях		
1	Классификация угроз в социальных сетях	Принципы работы злоумышленников в социальных сетях. Анализ профиля социальной сети с точки зрения злоумышленника
2	Методы защиты от угроз в социальных сетях	Методы защиты и управление настройками профиля в социальной сети
3	Кибербуллинг и доксинг	Что такое кибербуллинг и доксинг. Как противостоять злоумышленникам

Содержание программы

Тема 3. Социальная инженерия и методы защиты от неё		
1	Что такое социальная инженерия	Знакомство с основными сценариями и алгоритмами кибератак. Основы расследования киберпреступлений
2	Фишинг и антифишинг	Работы с фишинг атаками и подозрительными страницами, методы защиты электронной почты
3	Аудит паролей	Основные методы защиты от атак на пароли

Содержание программы

Тема 4. Управление инцидентами информационной безопасности. Технологии обнаружения компьютерных атак		
1	Обнаружение атак как механизм защиты	Методология защиты информации. Анализ и управление рисками, связанными с осуществлением сетевых атак
2	Уязвимости, угрозы и модели нарушителя	Классификация угроз и уязвимостей ИБ. Типы нарушителей и их классификация. Средства, используемые нарушителем. Модель Cyber-Kill Chain

Содержание программы

Тема 5. Обнаружение, анализ и расследование инцидентов информационной безопасности		
1	Средства обнаружения компьютерных атак	Виды систем обнаружений вторжений. История разработок СОВ. Классификация
2	Сетевой сенсор системы обнаружения атак ViPNet IDS NS	Основные функции и принцип работы программно-аппаратного комплекса ViPNet IDS NS
3	Сетевые атаки (вторжения)	Мониторинг событий в режиме реального времени. Просмотр журнала событий. Настройка отображения столбцов журнала
4	Поиск и анализ атак	Работа с журналом событий и атак. Анализ файлов в сетевом трафике на наличие вредоносного программного обеспечения. Мониторинг аномалий в поведении пользователей. Уровни важности событий информационной безопасности. Поиск событий с помощью фильтров. Группировка событий по параметрам. Работа с журналом событий и атак. Просмотр и поиск правил. Использование дополнительных вкладок для просмотра событий. Получение подробной информации о событии. Экспорт записей журнала событий

Содержание программы

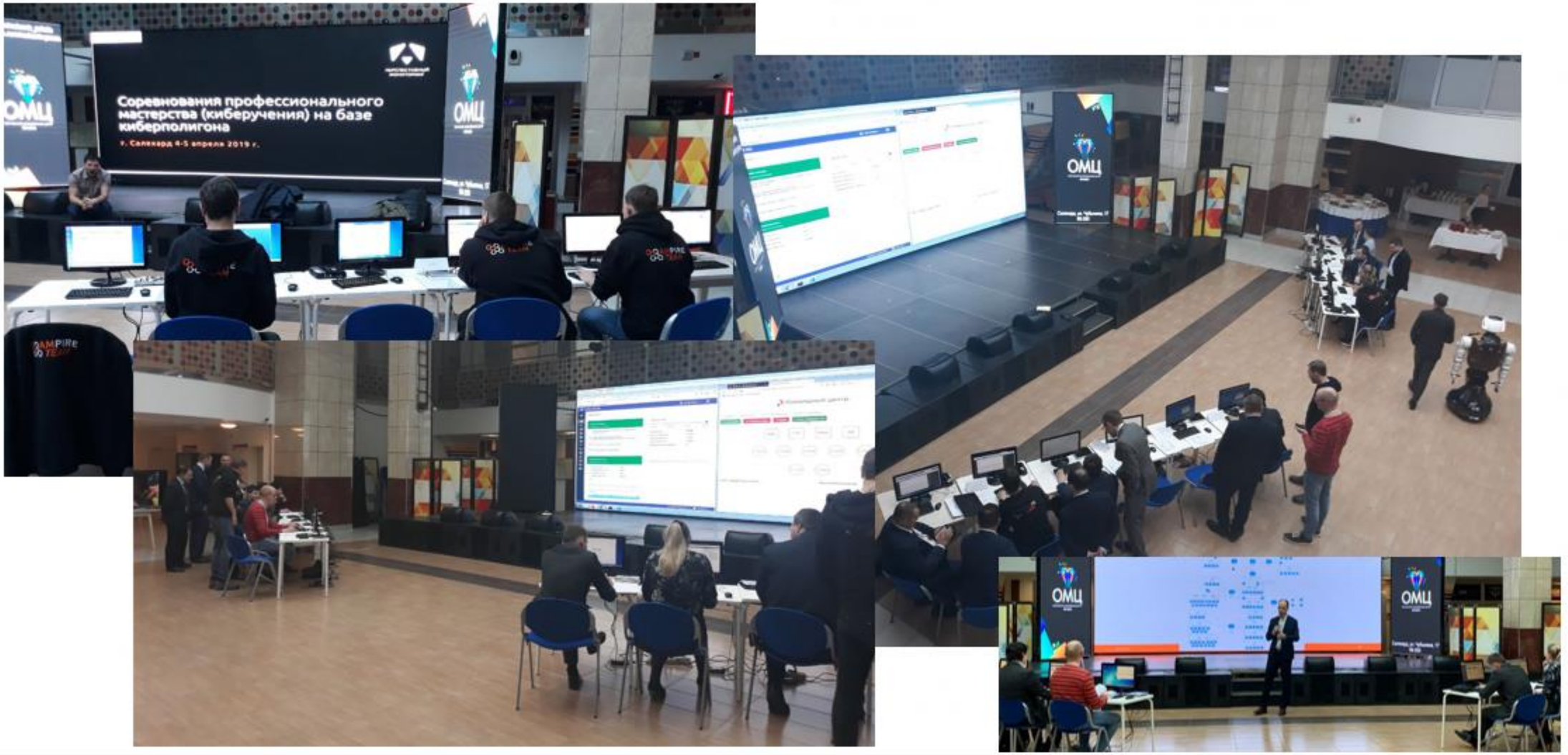
Тема 6. Обнаружение, анализ и устранение последствий компьютерных атак на базе программного комплекса «Ampire»		
1	Общие сведения об учебно-тренировочной платформе «Ampire»	Основное назначение ПК «Ampire», состав. Функциональные возможности. Типовой шаблон
2	Описание основного процесса проведения киберучений. Ролевая модель	Описание интерфейса ПК «Ampire». Распределение по группам. Панель тренировки. Статус уязвимостей. Группа мониторинга. Группа реагирования. Карточки инцидентов ИБ, создание и особенности заполнения. Cyber-Kill Chain
3	Отработка сценариев киберучений	Базовые сценарии
	Подключение к тренировке в составе команды группы мониторинга. Отработка сценария	Удаленное подключение к сетевому сенсору ПАК ViPNet IDS. Мониторинг, анализ и расследование инцидентов информационной безопасности. Просмотр и поиск записей журнала событий. Поиск инцидентов ИБ. Пошаговое отслеживание действий виртуального нарушителя в инфраструктуре предприятия. Экспорт файлов об инциденте. Создание карточки инцидента ИБ
	Подключение к тренировке в составе команды группы реагирования (защиты). Отработка сценария	Удаленное подключение к защищаемой сети. Работа в составе команды. Анализ и распределение карточек инцидентов ИБ. Пошаговый анализ действий виртуального нарушителя в инфраструктуре предприятия и их последствий, Выявление угроз безопасности информации и технических каналов утечки информации, обследование объекта ИС. Работа со специальным программным обеспечением для обнаружения и анализа событий ИБ. Устранение обнаруженных уязвимостей в ИС. Реализации защитных мер по устранению найденных недостатков ИБ

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

Киберучения



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Дмитрий Григорьев

Руководитель обособленного подразделения г. Новосибирск
АО «ИнфоТеКС

Dmitry.Grigoryev@infotecs.ru

Спасибо
за внимание!

Максим Кувшинов

Руководитель обособленного подразделения г. Новосибирск

АО «ПМ»

Maksim.Kuvshinov@amonitoring.ru

t.me/pm_public

amonitoring.ru