



КОНФЕРЕНЦИЯ КИБЕРПОЛИГОНОВ

Вместе против цифровой уязвимости

24 апреля
г.Москва, Кибердом



Ampire Keynotes

Нейгер Сергей

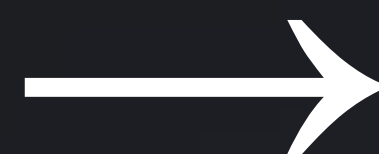
Мелихов Георгий

Худой Юрий

Цифры

Количество полигонов

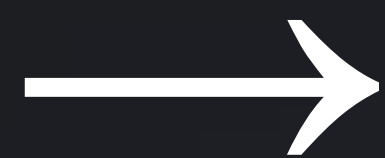
20
было



?

Количество полигонов

20
было



32
стало

Киберучения

500

киберучений



Вести-Смоленск

Подписаться

РОССИЯ 1
СМОЛЕНСК



ВЕСТИ СМОЛЕНСК

Преподаватели

300

преподавателей

Преподаватели

170

резюме

Вузы

2/3

заказчиков

Регионы

От Архангельска до Астрахани
От Калининграда до Хабаровска



Технологические партнёры



АСТРА

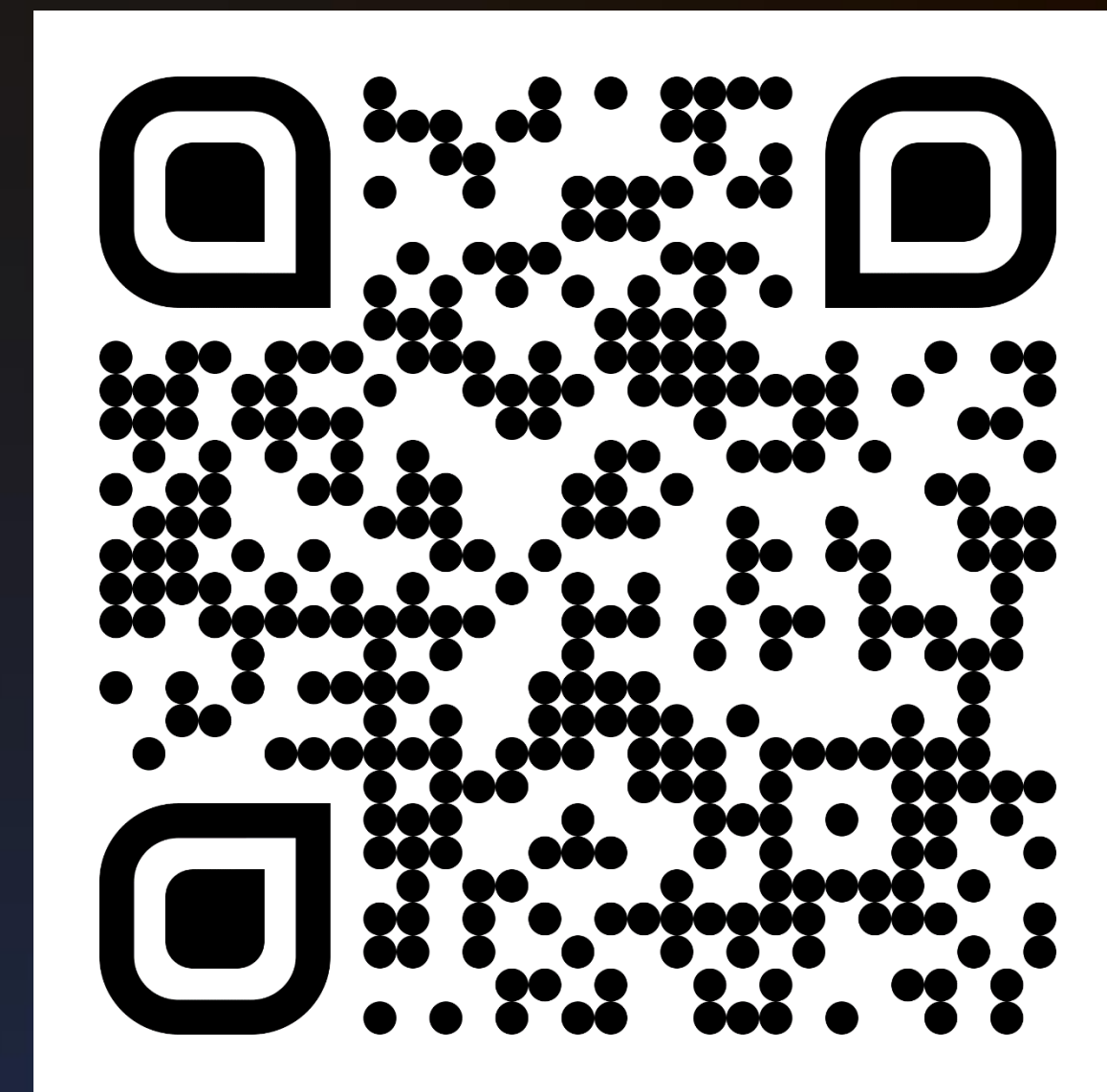


Сообщество Ampire

1 год работы

170 участников

2 примера интеграции



Продукт



Зрелый продукт

Влияние обратной связи на развитие продукта

The screenshot displays the 360° Ampire web interface, which is used for creating and managing cybersecurity training exercises. The interface is divided into several sections:

- Создание тренировки (Training Creation):** Located on the left, it shows progress through three steps: "Базовые настройки" (Basic settings), "Инфраструктура" (Infrastructure), and "Участники" (Participants). A dropdown menu for "Группа" (Group) is set to "Класс 10-Б". Below, a table lists participants with their names and avatars.
- Сгенерировать сценарий (Generate Scenario):** A modal window on the right allows users to create scenarios. It includes fields for "Название" (Name), "Сложность" (Difficulty), and "СЗИ" (Security Software). The "Сложность" dropdown is set to "Попроше" (Beginner). The "СЗИ" section has buttons for "SecOnion", "VIPNet IDS NS", and "VIPNet TIAS".
- Главная (Main Dashboard):** The central area shows statistics: "Активных тренировок" (Active trainings) at 1, "Тренировок пройдено" (Trainings completed) at 32, "Сценариев" (Scenarios) at 70, and "Шаблонов" (Templates) at 8. It also features sections for "Активные тренировки" (Active trainings) and "Последние сценарии" (Latest scenarios).
- OS удаленного рабочего места (Remote Workstation OS):** A dropdown menu at the bottom center shows the selection of an operating system for the remote workstation. The options are "Ничего не выбрано" (Nothing selected), "Windows 10", and "РЕД ОС 8" (Red OS 8), which is currently selected.
- Сайдбар (Sidebar):** On the right, the sidebar contains navigation links: "Главная" (Home), "Тренировки" (Trainings), "Сценарии" (Scenarios), "Конфигуратор" (Configurator), "Шаблоны" (Templates), "Группы и пользователи" (Groups and users), "База знаний" (Knowledge base), "Уведомления" (Notifications), "Настройки" (Settings), and a user profile for "Иванов Максим" (@ampire_teacher).

Пример 1

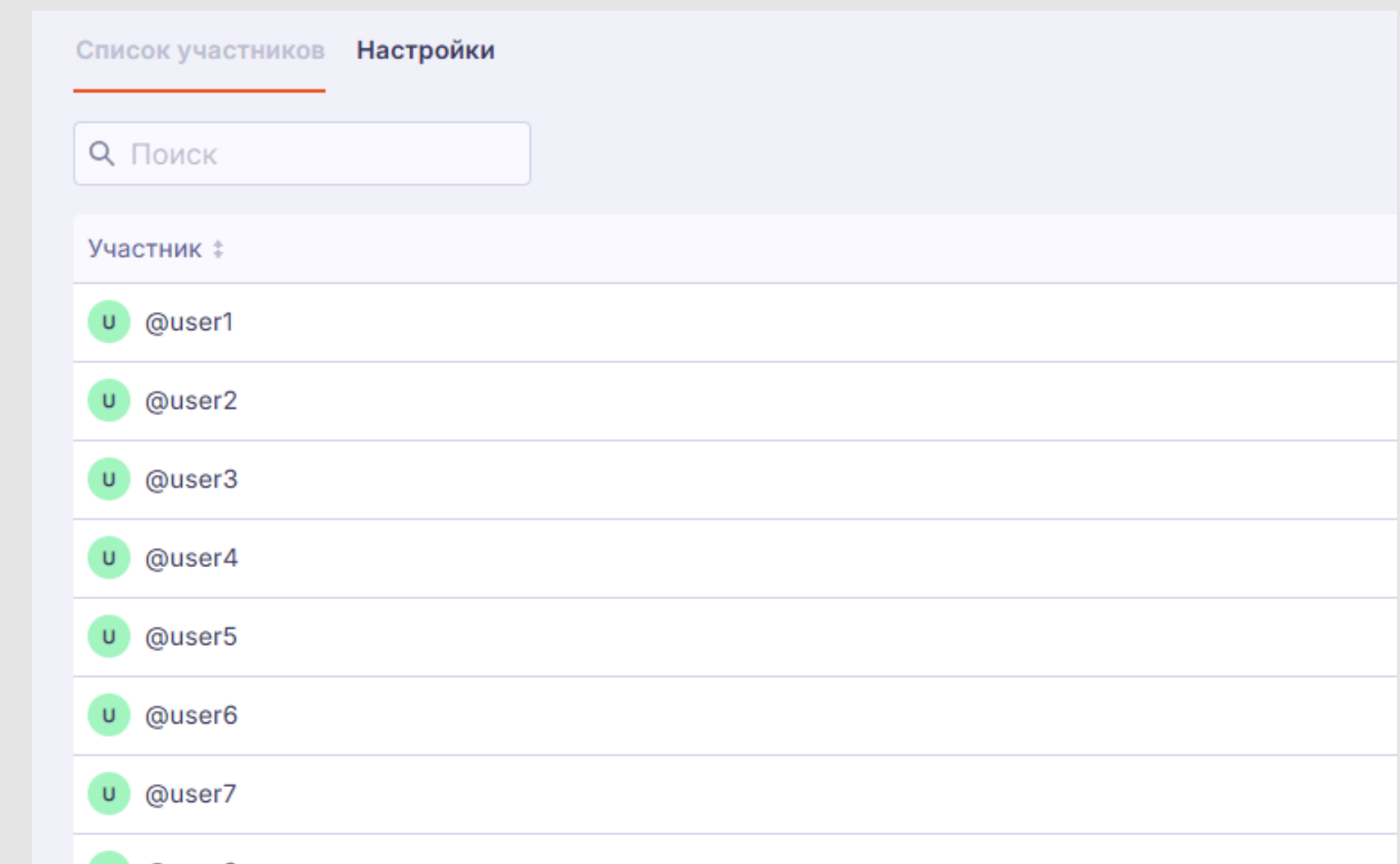
«Обезличенные учетки»

Проблемы:

- Для большого потока студентов долго заводить персональные учетные записи
- Иногда неизвестен состав участников киберучений, а подготовить тренировки требуется заранее

Решение:

- Возможность создавать учетные записи разных типов
- Универсальное отображение пользователей в интерфейсе



Пример 2

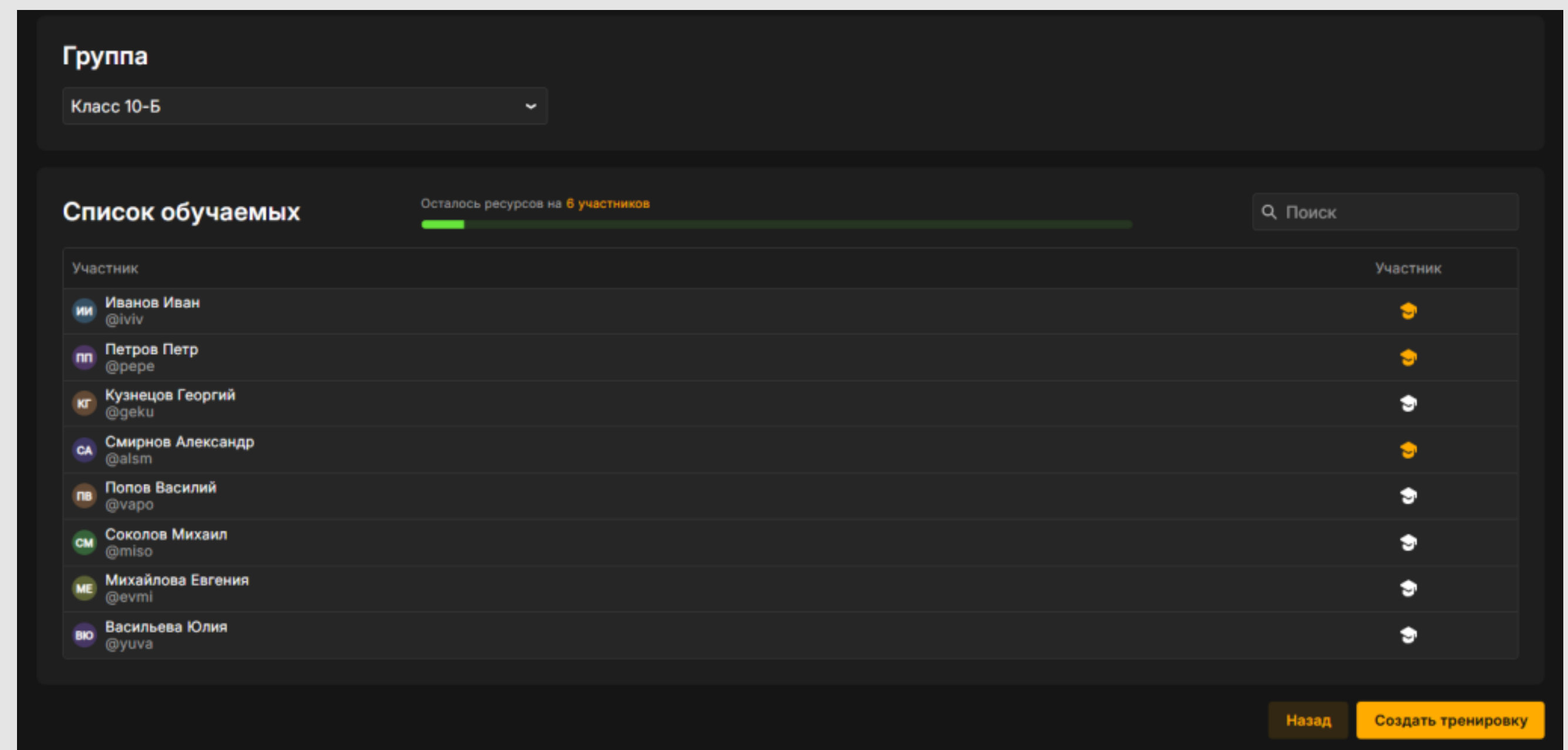
«Массовый Ampire Junior»

Проблема:

- Создавать вручную индивидуальные тренировки на большое количество человек долго и неудобно

Решение:

- Выбор нужных участников в один клик
- Сохранение за каждым участником индивидуального экземпляра инфраструктуры



Изменения за год

Уже доступно:

Отечественные
ОС в Ampire
Junior

Обновленный
дизайн и
улучшенные
шрифты

Счетчик активных
тренировок

Будет доступно в
версии 1.7:

Генератор
случайных
сценариев

Коробочные
сценарии на
конфигураторе

Контроль
ресурсов сервера



Разминка



admin@notify.vk.com

administrator@ampire-office.corp

Wed 11:59 PM

В Ваш аккаунт был выполнен вход с неизвестного устройства, Android, Moscow.

 При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.



Не удается отобразить связанный

Уведомление безопасности

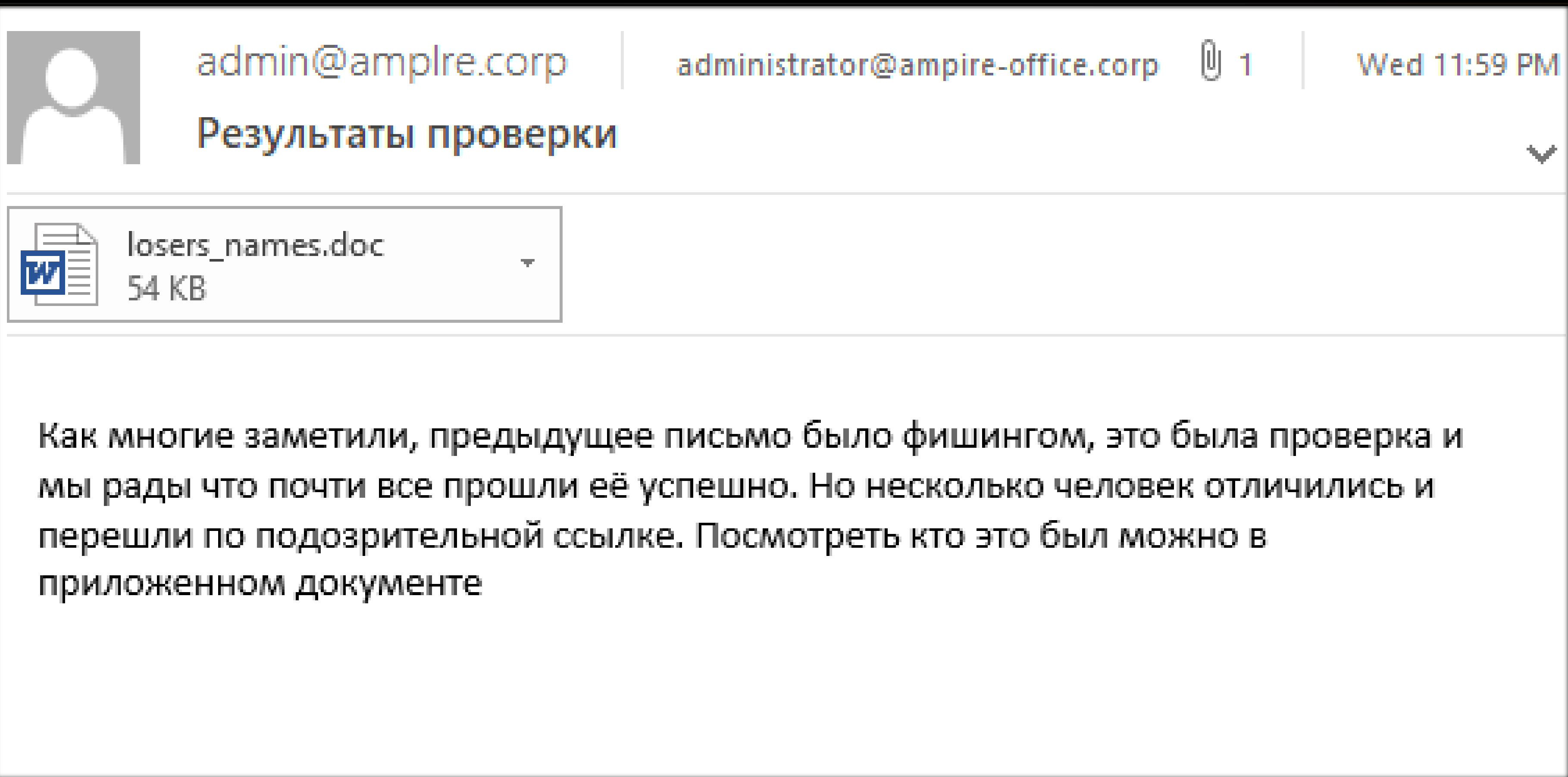
Вы получили это письмо, потому что в Ваш аккаунт был выполнен вход с неизвестного устройства.

Если это произошло с вами, пожалуйста, перейдите на свою страницу (vk.com), чтобы защитить свой аккаунт.

Желаем удачи,
Администрация ВКонтакте

Кликнули бы на эту
ссылку?

Разминка



Открыли
бы этот
файл?

Сценарии и шаблоны за год

Blue Team

Захват АРМ
администратора

Перехват
управления
контроллером
домена

Атака на РЗА и
другие сценарии

Red Team

Эксплуатация
Docker Escape

Захват интернет-
магазина
компании

Захват системы
хранения
больших данных

Ampire Junior

Cookies

GEOINT

Безопасные
пароли

Стеганография

Всего:

+16 новых
и +4
обновленных
уязвимых узла

+10
новых сценариев

+3
новых шаблона

Планы до конца 2026

	2025	2026
Форматы тренировок:	Red Team Labs OSINT Pro	Написание правил для СЗИ Red Team vs Blue Team
Интеграции:	Отечественные ОС SIEM	WAF
Сценарии и шаблоны:	Лабы на 40 мин (Ampire Junior) Новые интерактивные задания (Ampire Junior)	Конфигуратор Red Team Конфигуратор инфраструктуры

Разминка

Где сделано это фото?

- 1) Австралия
- 2) Канада





Ответ:

99 St NW, Edmonton, AB
T6E 1W6, Canada,

53.51806321399411,
-113.48616606455816

Ampire Junior – лабы на 40 мин

Цель – сделать лабораторные работы легко адаптируемыми под **любой** школьный урок

Федеральная рабочая программа | Информатика. 10–11

организация коллективного взаимодействия и обмена данными. Сетевой этикет: правила поведения в киберпространстве. Проблема подлинности полученной информации. Открытые образовательные ресурсы	Приводить примеры информационных... Характеризовать... образовательную... описывая имеюще... оснащение, прогр... и их использовани...
	веб-сайта. Структура адресов веб-ресурсов. Браузер. Поисковые системы. Поиск информации по ключевым словам и по изображению. Достоверность информации, полученной из Интернета. Современные сервисы интернет...

Лабораторная работа
на базе ФРП

Сценарии (II и III квартал 2025):

- Поисковые системы и службы – поиск по ключевым словам и изображениям
- Сетевой этикет и стратегии безопасного поведения в Интернете
- Достоверность информации, полученной из Интернета
- Деструктивные формы сетевой активности – кибербуллинг
- Защита личной информации в Интернете
- Геоинформационные системы – поиск информации по изображению

Универсальность Ampire

Специалисты ИБ

Разработчики СЗИ

Школьники

Непрофильные
специалисты



Специалисты ИТ

Начинающие специалисты

Разработчики и DevOps

Отраслевые специалисты

Техника

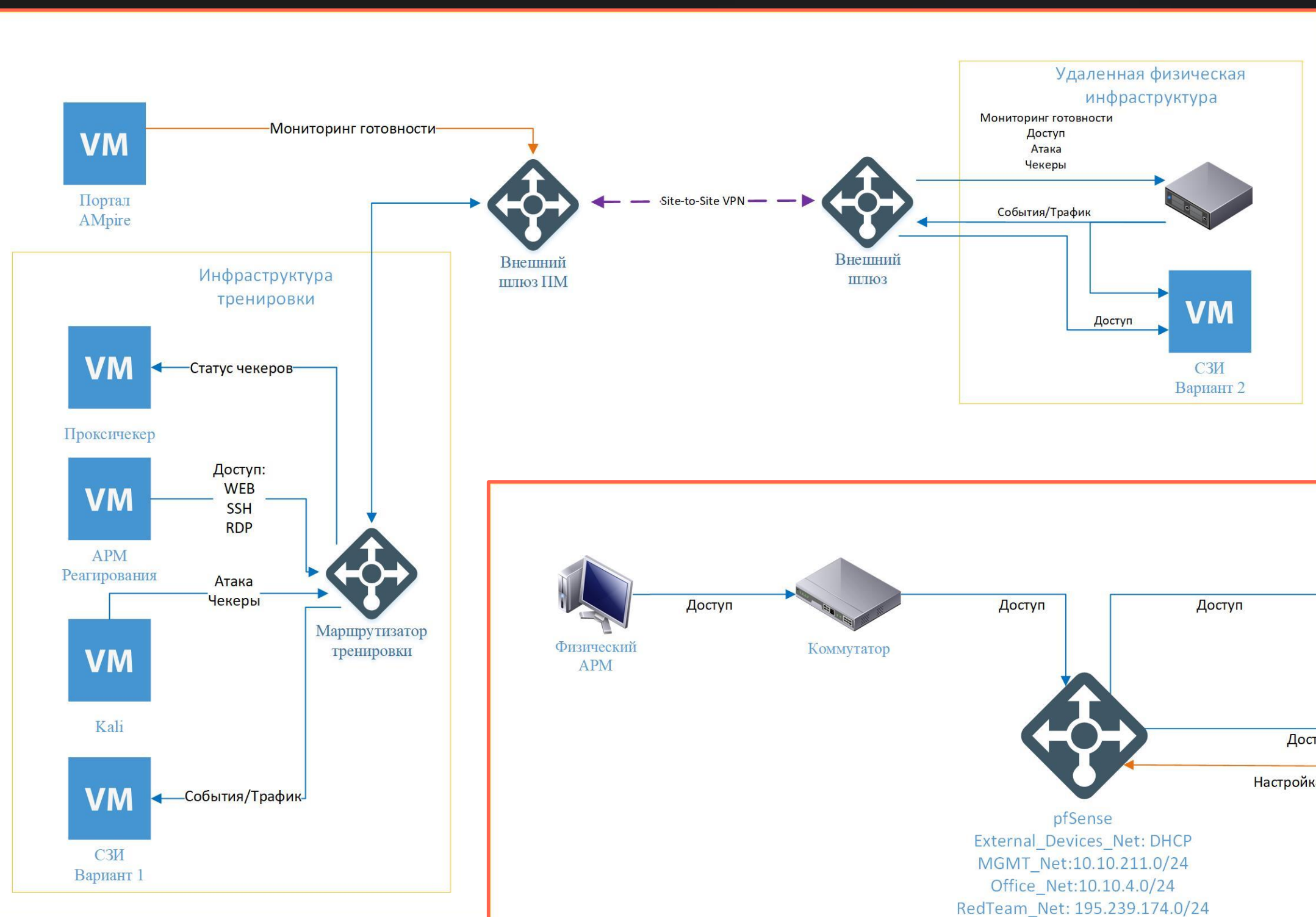
Импортозамещение

Что нам нужно от виртуализации:

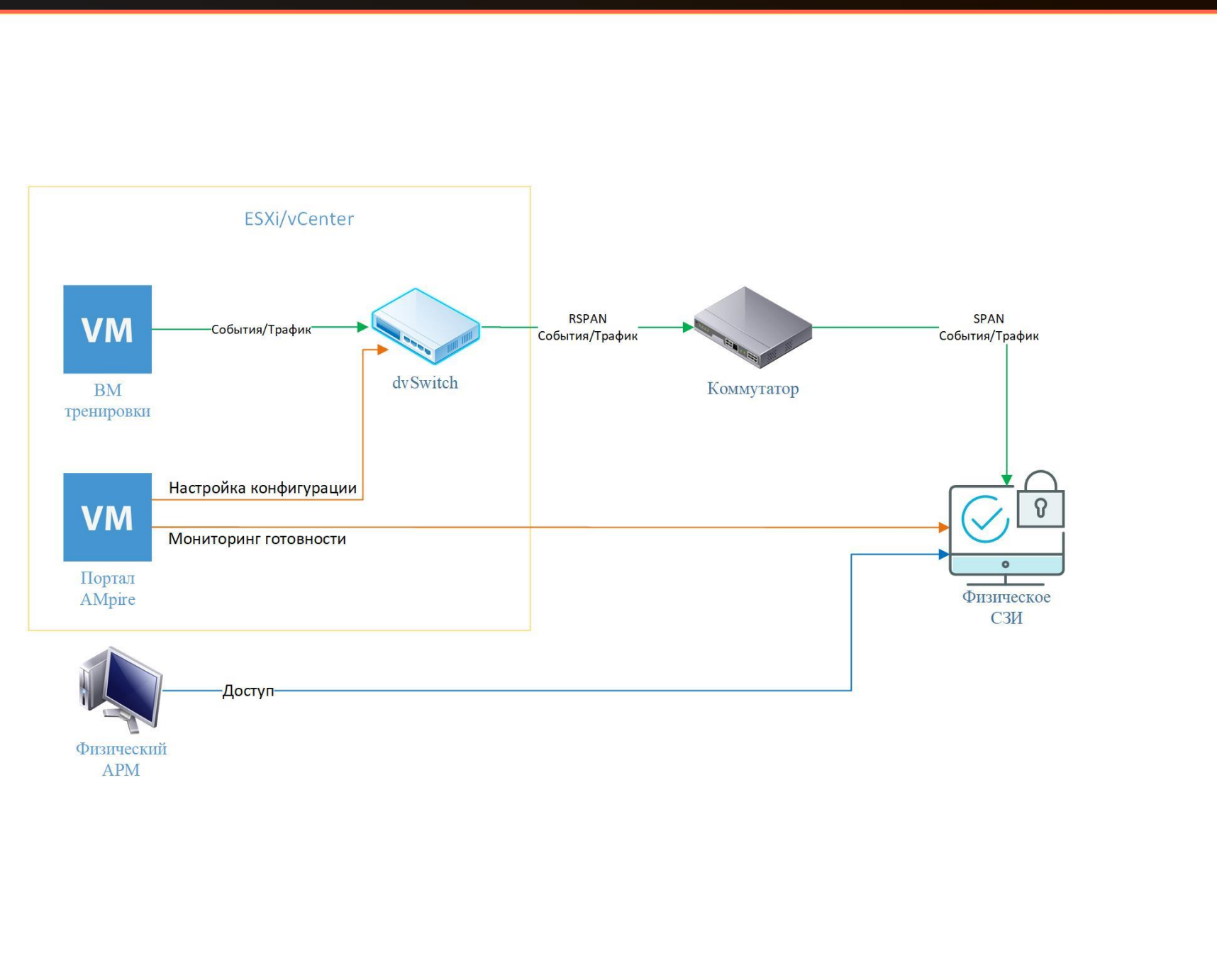
- Стабильная работа VM Windows/Linux
- Автозапуск VM после включения сервера
- Поддержка блочного СХД
- Кластер в режиме High Availability
- Холодная и горячая миграция VM
- Поддержка тонких дисков
- Создание снапшотов
- Поддержка распределенного виртуального коммутатора

Киберфизические стенды

Удаленная инфраструктура



Физическое СЗИ



← **Физический АРМ**

Мониторинг готовности шаблона



Узел AMpire_ST_Enterprise_PR1_InternalGW

1. Проверка ответа 200 от <https://10.10.2.254>;
2. Проверка состояния интерфейсов:
 - em0 (DMZ_Net)
 - em1 (DC_Net)
 - em2 (Dev_Net)
 - em3 (ASU_Net)
 - em4 (Office_Net)

Узел AMpire_ST_Enterprise_PR2_DC_FS

1. Проверка портов: 445 (SMB), 3389 (RDP);
2. Проверка работы сервисов:
 - Terminal Services (TermService) (RDP)
 - DNS Client (Dnscache)
 - Storage Service (StorSvc)
 - ViPNet EPP Agent (EPPService)
 - ViPNet EPP Controller (EPPController)
 - ViPNet EPP Net Sensor (SnortSvc)
 - winlogbeat (winlogbeat)
 - Systemfsms (Systemfsms)

Узел AMpire_ST_Enterprise_PR1_DC_Mail

1. Проверка портов: 43 (DNS), 993 (IMAP), 3389 (RDP);
2. Проверка работы сервисов:
 - IIS Admin Service (IISADMIN)
 - Microsoft Exchange IMAP4 (MSExchangeImap4)
 - Microsoft Exchange IMAP4 Backend (MSExchangeIMAP4BE)
 - DNS Client (Dnscache)
 - Remote Desktop Services (TermService)
 - ViPNet EPP Agent (EPPService)
 - ViPNet EPP Controller (EPPController)
 - ViPNet EPP Net Sensor (SnortSvc)
 - winlogbeat (winlogbeat)

Узел AMpire_ST_Enterprise_PR1_UO_Insider

1. Проверка работы сервисов:
 - ssh.service
 - msfrpcd.service
 - sc8_xss_check.service

Стабильность

Система доставки и применения обновлений контента





Благодарим за внимание!

