Национальный киберполигон

Основной инструмент проверки кибербезопасности России

Ростелеком

Национальный киберполигон

Это «виртуальная страна» с реалистичными инфраструктурами предприятий ключевых отраслей российской экономики

- Техническая инфраструктура с настоящим отраслевым оборудованием
- Специализированный программный комплекс для проведения киберучений
- Уникальная методика обучения специалистов с учетом их знаний и специфики отрасли

Цели создания киберполигона

Ростелеком

Киберучения

Первоочередная задача киберполигона – это проведение масштабных киберучений для отработки практических навыков реагирования на новейшие атаки. Регулярные киберучения повышают готовность к атакам преступников и обеспечивают национальную безопасность страны.

Органы государственной власти

- Киберучения национального масштаба
- Оценка готовности ведомств к отражению атак
- Разбор реагирования на кибератаки

Корпорации и предприятия

- Обучение персонала новым технологиям и инструментам для более эффективного отражения атак в реальном времени
- Повышение квалификации и поддержка мотивации ИБ-специалистов

Образовательные учреждения

- Повышение уровня осведомленности о киберугрозах
- Обучение защите от компьютерных атак
- Объективная оценка уровня знаний

Оценка и развитие практических навыков

На киберполигоне эмулируется типовая инфраструктура выбранной отрасли, включая сетевую часть, конкретные сервисы, приложения, инструменты и т. д.

Это дает возможность:

- на практике освоить лучшие средства и методы защиты информации
- подготовиться к реальным актуальным атакам
- научиться защищаться от атак в реальном времени
- объективно оценить уровень знаний специалистов
- выявить и закрыть уязвимости инфраструктуры

На такой эмулированной площадке можно безопасно тренировать специалистов во время наиболее актуальных и деструктивных атак, отрабатывать навыки реагирования на инциденты, анализа защищенности, обнаружения компьютерных атак и защиты от них, работы в команде, оттачивать мастерство Blue- и Red-команд, а также рядовых ИБ-специалистов.

Проверка безопасности информационных и промышленных систем

- **Лаборатория по тестированию ПО и программно-аппаратных комплексов.** Исследования на уязвимости, программы bugbounty, тестирование программ по разным направлениям
- DevSecOps&SDL. Обучение применению практикам безопасного развертывания ПО

Киберполигон для всей страны

Ростелеком

Федеральные и региональные органы исполнительной власти

Развитие экспертизы своих ИБ-специалистов на площадке государственного уровня для защиты от киберугроз, выполнения требований к обучению персонала и повышения осведомленности.

Коммерческие и государственные предприятия

Эмуляция кибератак на платформе киберполигона позволяет развить навыки существующих специалистов и подготовиться к защите от компьютерных атак, не рискуя производственными и бизнес-процессами.

Университеты

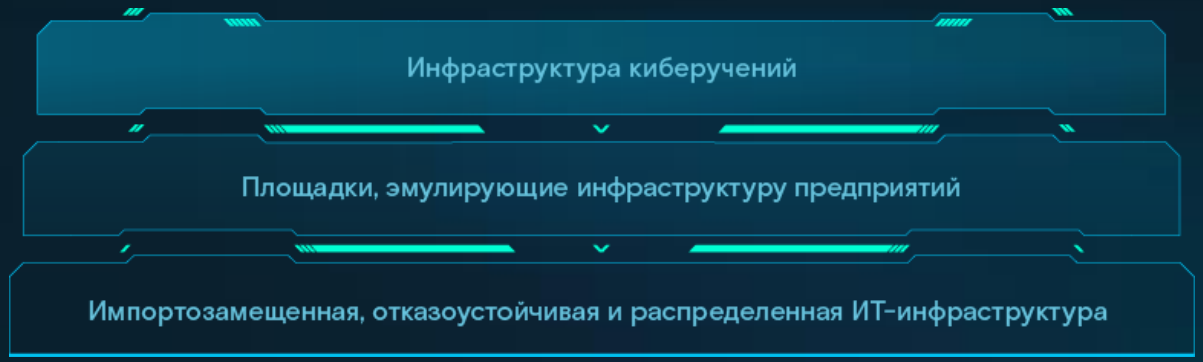
Актуальные знания о «горячих» киберугрозах для студентов и преподавателей в формате интенсивного, интерактивного и геймифицированного практикума.

Устройство киберполигона

Ростелеком

Как устроен киберполигон

Киберполигон – это комплекс аппаратных и программных решений с эмулируемыми инфраструктурами, которые работают на платформе с функциональным и удобным интерфейсом.



Отраслевые сегменты:
- промышленность
- банки
- энергетика
- телеком
- и т. д.

Инфраструктура сегментов максимально приближена к реальной. Соревнования и тренировки, занятия и киберучения проходят на отдельных платформах через веб-портал.

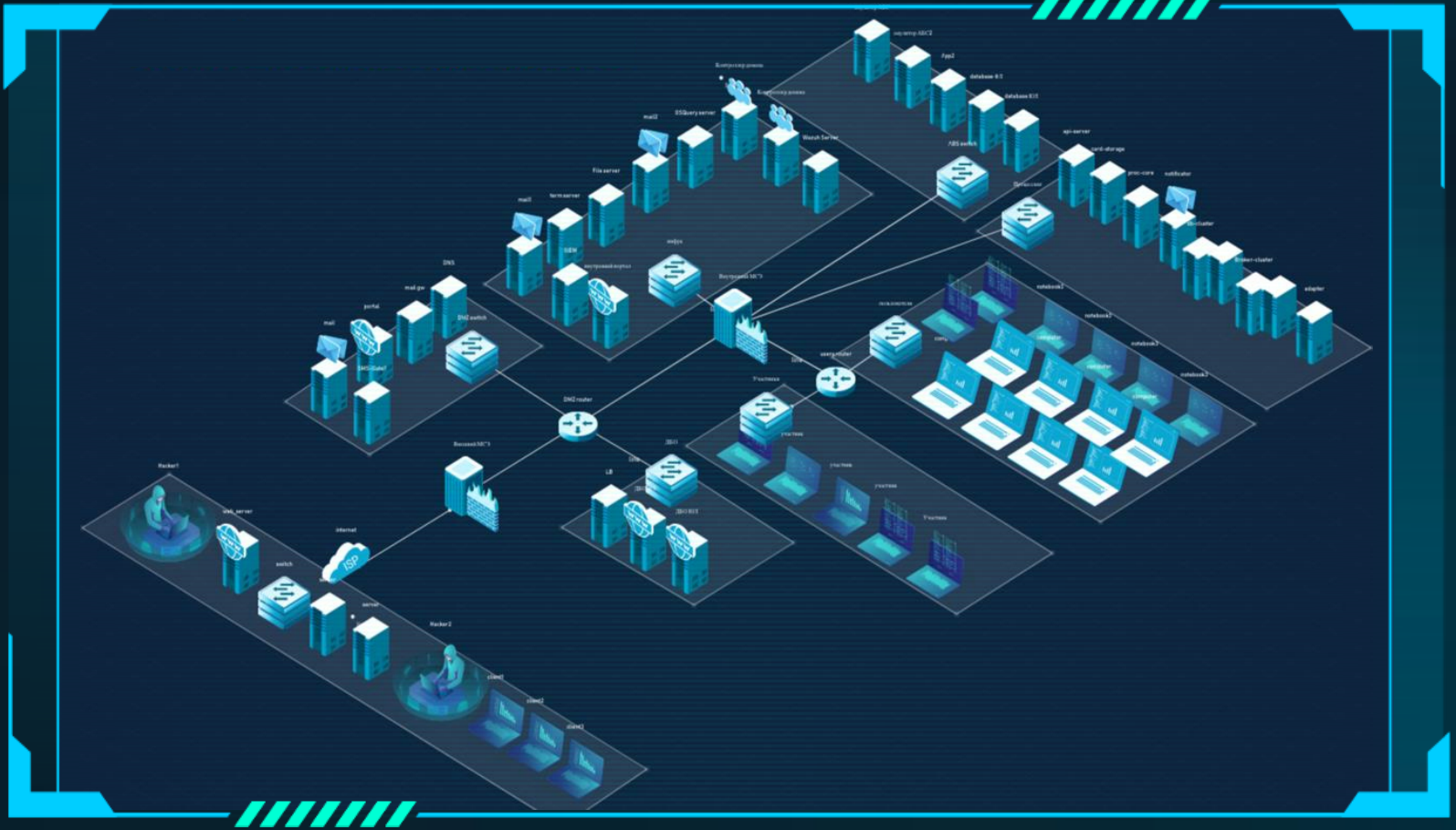
Как устроен киберполигон

В рамках киберполигона реализуются отраслевые инфраструктуры

Корпоративный сегмент	Электроэнергетика	Банковский сектор
Имитация офисной инфраструктуры: рабочие станции, почтовые и веб-серверы, корпоративные средства защиты и т. д.	Эмуляция систем релейной защиты, автоматики, мониторинга переходных процессов и диспетчерского управления с применением реальных компонентов АСУ ТП	Воспроизведение типичной ИТ-инфраструктуры финансовой организации, в том числе систем банковского обслуживания и процессинга

Схема промышленной инфраструктуры

Схема банковской инфраструктуры



Планы развития

Ростелеком

Планы на 2020-2021 гг.

	Сегодня	К концу 2021
Киберучения	4	14+
Обученные специалисты	100+	450+
Сегменты	Корпоративный офис Передача электроэнергии Финансовый сектор	Добыча нефти и газа Транспортировка нефти и газа Генерация электроэнергии
Опорные пункты	Сириус о. Русский Москва	Санкт-Петербург

Дорожная карта развития на 2020–2024 гг.

2020

Подготовка инфраструктуры

Оборудование

- 20 серверов
- Отраслевое оборудование
- Отраслевое ПО
- СЗИ

Базовый блок

- Киберучения
- База скриптов атак
- Конструктор атак

Покрытие отраслей КИИ

- Корпоративный офис
- Кредитно-финансовый сектор
- Электроэнергетика

2021

Новые возможности

- Защита от распространенных атак
- Этичный хакинг
- База скриптов типовых процессов ИБ

Покрытие отраслей КИИ

- Добыча нефти и газа
- Транспортировка нефти и газа

2022

Новые возможности

- Red Teaming
- Противостояние команд
- Пентестеры

Услуги для регуляторов

- Киберучения на соответствие ГосСОПКА
- SOC Training
- Архитекторы SOC

2023–2024

Услуги для заказчиков

- Учения для руководителей
- Глобальные межотраслевые учения

Покрытие отраслей КИИ

- Телекоммуникации
- Транспорт
- Металлургия

Уникальность национального киберполигона

Отраслевое оборудование и ПО

Инфраструктуры киберполигона максимально приближены к инфраструктурам реальных компаний

Национальный масштаб

Среди ключевых партнеров – Центральный Банк России, ведущие вендоры и учебные учреждения

Мультиотраслевая направленность

Постоянное расширение видов отраслей позволяет закрывать потребности большинства основных организаций страны и проводить кросс-отраслевые учения

Уникальные методики

Единая матрица навыков адаптирована для учащихся разного уровня и из разных отраслей

Доступность 365 дней в году

За счет встроенных шаблонов типовых предприятий нет необходимости разворачивать и настраивать инфраструктуру с нуля

Удаленный доступ к тренировкам

Удаленный доступ делает киберполигон доступным даже в условиях дистанционной работы и обучения.

Киберполигон создан при участии

Минцифры России

Министерство энергетики Российской Федерации

Банк России

Сириус

ДВФУ Дальневосточный федеральный университет

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком