ПРОЕКТ

Тренинг Международного союза электросвязи «Безопасность провайдерских сетей. Защита критической инфраструктуры в современных условиях»

БГУИР, г. Минск, Республика Беларусь, 13-17 октября 2025 г.

ПРОГРАММА МЕРОПРИЯТИЯ

13 октября 2025 Введение в безопасность провайдерских сетей	
09:00–09:25	Регистрация участников
09:25–09:30	Открытие тренинга
09:30–10:15	Современные угрозы и вызовы в сетях операторов
10:15–11:00	Эволюция кибератак: от простых сканеров до сложных многоэтапных атак (APT)
11:00–11:10	Перерыв
11:10–12:30	Роль провайдера в защите своих клиентов
12:30–12:40	Перерыв
12:40–14:00	Важность защиты собственной инфраструктуры
14 октября 2025 Защита инфраструктуры операторов связи	
09:30–10:15	Создание выделенной сети управления и защита активного сетевого оборудования
10:15–11:00	Организация сети управления для серверной инфраструктуры и хранилищ данных
11:00–11:30	Архитектура защищённой сети управления
11:30–11:40	Перерыв
11:40–12:30	Реализация на практике и кейсы зрелых провайдеров
12:30–12:40	Перерыв
12:40–14:00	Обсуждение: как адаптировать модели защиты
15 октября 2025 IPS/IDS и Honeypot-системы	
09:30–10:00	Принципы работы Intrusion Prevention и Detection Systems
10:00–10:40	DPI (Deep Packet Inspection) как основной инструмент анализа трафика
10:40–10:50	Перерыв
10:50–11:20	Настройка политик IPS
11:20–11:30	Перерыв
11:30–11:50	Цель Honeypot-систем
11:50–12:10	Основные задачи Honeypot
12:10–12:20	Типы Honeypot
12:20–12:50	Рекомендации по внедрению Honeypot
16 октября 2025 BGP и защита от DDoS	
09:30–10:00	Типовые атаки на BGP
10:00–10:30	Механизмы защиты
10:30–10:40	Перерыв
10:40–11:00	Успешные примеры предотвращения BGP-угонов
11:00–11:10	Перерыв
11:10–11:20	FlowSpec, Anycast, реальные инциденты и анализ кейсов
11:20–11:50	Типы DDoS-атак и их влияние на оператора
11:50–12:30	Архитектуры защиты от DDoS
12:30–13:00	Использование BGP FlowSpec для фильтрации трафика
13:00–13:30	Примеры реальных DDoS-атак на провайдеров и их последствий

17 октября 2025 Трафик, IPv6 и критические сервисы	
09:30–10:15	Использование NetFlow, sFlow и IPFIX для анализа трафика
10:15–11:00	Выявление аномалий с помощью систем машинного обучения
11:00–11:10	Перерыв
11:10–11:50	Особенности IPv6, влияющие на безопасность
11:50–12:20	Угрозы в IPv6-сетях
12:20–12:50	Меры безопасности
12:50–13:10	Практическое использование IPv6 для повышения безопасности
13:10–13:30	Безопасность DNS
13:30–14:00	DHCP Snooping и предотвращения MITM-атак
14:00–14:20	Аутентификация NTP для защиты от подмены времени
14:20–14:30	Подведение итогов. Закрытие тренинга

КОНТАКТЫ ОРГАНИЗАТОРОВ

Белорусский государственный университет информатики и радиоэлектроники
отдел маркетинга и научных коммуникаций: тел.: +375445000533, email: science@bsuir.by
Подробнее о тренинге на сайте