360° Ampire

КОНФЕРЕНЦИЯ КИБЕРПОЛИГОНОВ

Вместе против цифровой уязвимости

24 апреля

г.Москва, Кибердом

Программа переподготовки: Противодействие киберугрозам в энергетической отрасли с использованием киберполигона Ampire

Григорьева Ирина Васильевна,
ст.преподаватель

Янова Ольга Юрьевна,
доцент

ФГБОУ ВО «КГЭУ»

Основные цели обучающей программы

Ampire 360°

Подготовка специалистов для выявления и предотвращения основных киберугроз, характерных для энергетических предприятий и инфраструктуры отрасли

Развитие компетенций по проектированию и совершенствованию стратегий киберзащиты с учётом актуальных методов атак и требований отрасли

Освоение практических навыков реагирования на киберинциденты и восстановления работоспособности критических объектов с применением реальных сценариев

Роль энергетической инфраструктуры в современной экономике

1. Энергетическая инфраструктура является фундаментом функционирования промышленных, транспортных и бытовых систем. Любой сбой в её работе приводит к нарушению производственных процессов и жизнедеятельности.

2. Сохранение бесперебойной работы энергосистем важно для социальной стабильности страны. Защита энергетики напрямую отражается на национальной безопасности населения и конкурентоспособности экономики.

Ampire 360°

Кибербезопасность в энергетике: вызовы и новая реальность

Энергетика становится главной целью кибератак, и защита отрасли приобретает первостепенное значение. Рост числа инцидентов угрожает экономике, безопасности и стабильности общества, требуя специализированной подготовки и практического опыта специалистов

Основные направления угроз в энергетике

Атаки на SCADA и интеллектуальные сети (Smart Grid)

Инфраструктурные атаки на SCADA и Smart Grid затрагивают системы управления, нарушая стабильную подачу энергии и работу оборудования. Такие инциденты усугубляются цифровизацией энергопредприятий.

Вредоносное программное обеспечение в энергетике

Вредоносное ПО используется для саботажа, сбора информации или уничтожения данных. Проникновение в энергообъекты зачастую приводит к частичному или полному выводу оборудования из строя.

Релейная защита

это система автоматического обнаружения и отключения повреждённого оборудования в энергосети для:

- Предотвращения аварийного развития ситуации
- Минимизации ущерба оборудованию
- Обеспечения надёжности электроснабжения

Атака	Последствия
Подмена данных с датчиков	Ложные срабатывания/неотключения
Взлом уставок защиты	Некорректная работа алгоритмов
Блокировка срабатываний	Отказ защиты при аварии
Манипуляция GOOSE-сообщениями	Нарушение логики работы

Ampire 360°

Инциденты в отрасли: примеры и последствия

Крупные отключения энергоснабжения

Волна атак в Восточной Европе привела к массовым отключениям электроэнергии, затронув миллионы потребителей и нарушив работу городской инфраструктуры.

Атаки на добывающие предприятия

Инциденты в нефтегазовой отрасли завершались временной остановкой стратегического оборудования и срывом поставок сырья на экспорт.

Пожары и технологические сбои

Вредоносные программы вызвали воспламенение трансформаторов, что повлекло за собой значительные материальные убытки и опасность для персонала.

Раскрытие критичных уязвимостей

Проведённые атаки выявили масштабные уязвимости в системах управления, что потребовало срочных мер по совершенствованию защиты энергообъектов.

Рост числа кибератак на объекты критической инфраструктуры (2019-2025)

Динамика демонстрирует ежегодное увеличение числа кибератак, особенно в сфере энергетики. Современные киберугрозы требуют своевременной переподготовки специалистов.

Постоянный рост атак указывает на необходимость регулярного повышения квалификации сотрудников для защиты критических объектов энергетики

Ampire 360°

Целевая аудитория программы

Продвинутый курс

Технические специалисты IT-направления в энергокомпаниях

Специалисты в области информационных технологий, заинтересованные в углублённом изучении защиты инфраструктуры энергетики и внедрении современных решений в промышленной среде.

Инженеры, отвечающие за обеспечение безопасности данных и систем в энергетических компаниях, желающие повысить квалификацию для противодействия новым киберугрозам.

Базовый курс

Рядовые сотрудники в энергокомпаниях

Работники электростанций, сетевых и генерирующих предприятий, чьи задачи связаны с эксплуатацией технологических комплексов и минимизацией рисков сбоев и атак.

Молодые профессионалы и студенты профильных вузов, стремящиеся освоить навыки анализа угроз и построения стратегий защиты критических объектов.

Структура обучения: теория и практика на киберполигоне Ampire

Теоретическая часть ориентирована на разбор современных угроз, особенностей инфраструктуры энергетики и построение надёжных систем киберзащиты. Содержит анализ уязвимостей и принципов противодействия современным типам атак.

Практический модуль включает работу на киберполигоне Ampire, где слушатели моделируют реальные атаки, осваивают сценарии реагирования и внедряют комплексные решения для защиты критических объектов энергетики.

Ampire 360°

Ключевые темы теоретического обучения

Актуальные угрозы

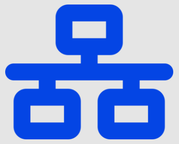
Разбор современных киберугроз, нацеленных на энергетические предприятия, с детальным рассмотрением методов и мотивов атакующих, используемых сценариев и последствий реализованных инцидентов.

Уязвимости систем

Анализ уязвимых мест в системах управления и IT-инфраструктуре, методов их выявления, а также событий, связанных с эксплуатацией известных и новых технических недостатков.

Методы защиты

Изучение передовых методов и инструментов для защиты инфраструктуры энергетики: от периметровой обороны до средств обнаружения вторжений и реагирования на инциденты.



Требования к критическим объектам

Ознакомление с требованиями к безопасности энергетической инфраструктуры, стандартами и нормативами, а также порядком обеспечения непрерывности функционирования объектов.

Примеры кейсов по кибербезопасности объектов энергетической инфраструктуры

1. Body Несанкционированный доступ к SCADA через слабый пароль
2. Фишинговая рассылка для инженеров подстанции
3. DDoS-атака на веб-портал энергокомпании
4. Внедрение вредоносного ПО через USB-носитель
5. Атака на IoT-сенсоры в распределённой сети
6. Перехват управления системой резервного питания
7. Утечка конфиденциальной информации через облачные сервисы
8. Социальная инженерия для получения доступа к подстанции
9. Нарушение сегментации сети между ИТ и ОТ
10. Атака на систему мониторинга энергопотребления с использованием вредоносных обновлений

Ampire 360°

Практические тренировки на киберполигоне: этапы и задачи

01

На киберполигоне Ampire участники отрабатывают моделирование актуальных кибератак на энергетическую инфраструктуру в условиях, приближённых к реальным. Каждый сценарий построен на основе анализа распространённых методов атак.

02

В ходе тренировки осуществляется пошаговая отработка реагирования: от обнаружения нарушения до нейтрализации угрозы и восстановления технологических процессов. Это формирует практические навыки оперативной защиты.

Ampire 360°

Григорьева Ирина Васильевна

@IRINA_V_GRIGOREVA

Янова Ольга Юрьевна

ianova.oiu@kgeu.ru

@OLE4KAYUREVNA

360° Ampire

Благодарим за внимание!