Кибербезопасность в энергетике

Докладчик:

Евгений Дружинин

КРОК

Автор:

Евгений Леонидович Дружинин,

ведущий эксперт по информационной безопасности, к.т.н.

ЗАО «КРОК инкорпорейтед»

Кибербезопасность в энергетике

Источник: *Мелких А.А., Микова С.Ю., Оладько В.С. Исследование проблемы информационной безопасности АСКУЭ // Universum: Технические науки*

Кибербезопасность в энергетике

КИБЕРАТАКА НА ГИДРОЭЛЕКТРОСТАНЦИЮ (ВЕНЕСУЭЛА)

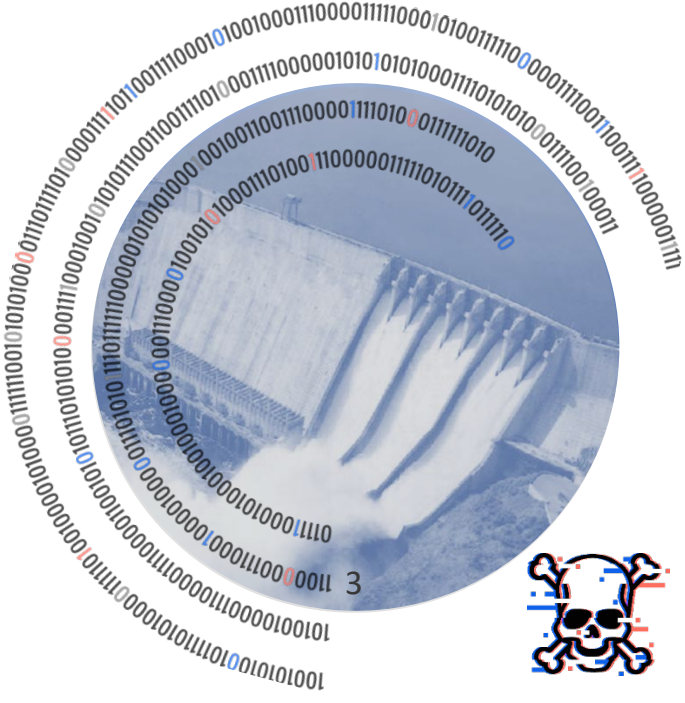
Объект воздействия –
гидроэлектростанция «Эль-Гури»

Суть инцидента –
обесточивание аэропорта, метро, отключение света

Территориальный охват –
Каракас и двадцать штатов Венесуэлы

Источник воздействия –
не выявлено

Год проведения атаки –
2019



Кибербезопасность в энергетике

КИБЕРАТАКА НА NORSK HYDRO

Объект воздействия –
производитель алюминия Norsk Hydro

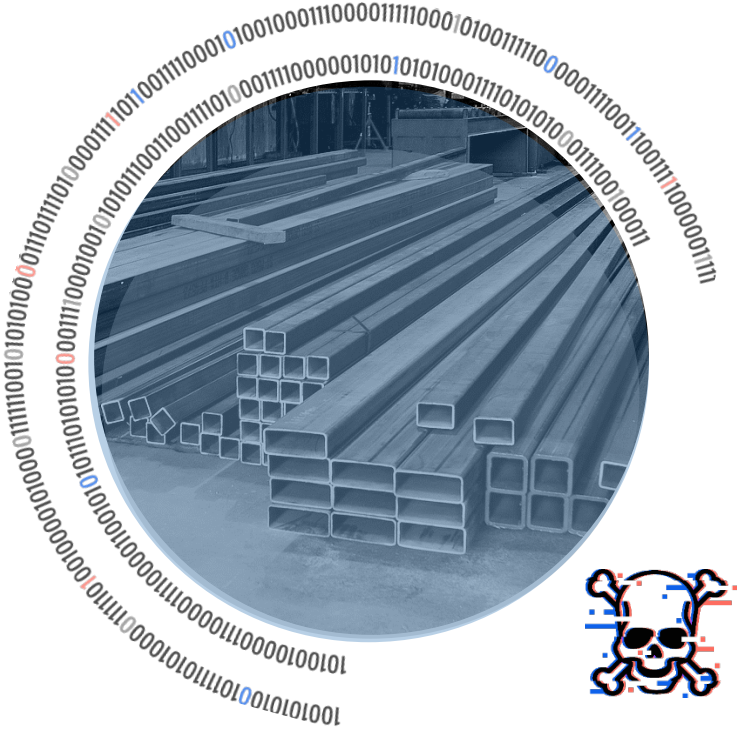
Суть инцидента –
сбой в работе производственных объектов из-за вымогательского ПО LockerGoga

Территориальный охват –
Норвегия, Катар и Бразилия

Источник воздействия –
не выявлено

Год проведения атаки –
март 2019

Финансовый ущерб (1 квартал) –
300-350 миллионов норвежских крон



Кибербезопасность в энергетике

КИБЕРАТАКА НА SAUDI ARAMCO

Объект воздействия –
нефтеперерабатывающий завод в Саудовской Аравии

Суть инцидента –
отключение инфраструктуры с использованием вредоносного ПО, предполагался взрыв и человеческие жертвы

Источник воздействия –
предположительно иностранные спецслужбы

Год проведения атаки –
2016 (расследование продолжается)

Кибербезопасность в энергетике

КИБЕРАТАКА НА АЗС

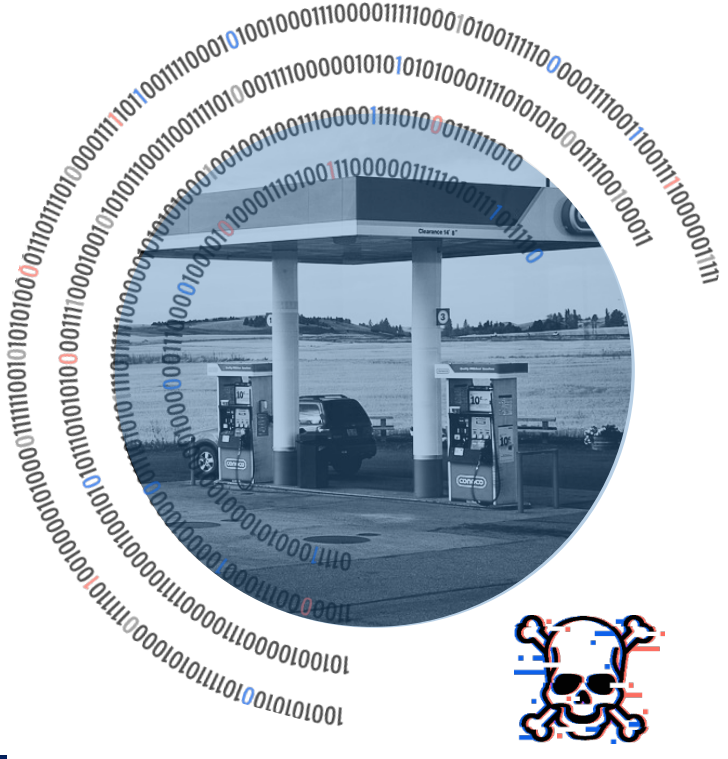
Объекты воздействия –
компоненты АЗС (колонки, счетчики, средства кассового учета)

Суть инцидента –
недолив топлива клиентам АЗС

Территориальный охват –
Юг РФ (Ставрополь, Краснодар, Северный Кавказ)

Источник воздействия –
хакер Денис Заев и сотрудники АЗС

Год обнаружения –
2018



Кибербезопасность в энергетике

ВЫВОДЫ

- Киберриски и объекты воздействия многообразны
- Затрагивают объекты критической информационной инфраструктуры, в том числе в сфере энергетики
- Последствия реализации очень критичны (экология, обеспечение жизнедеятельности и безопасности людей, обороноспособность страны, воздействие на политическую ситуацию)
- Требуется всесторонний анализ киберрисков и реализация систем безопасности

Кибербезопасность в энергетике

ПРЕДПОСЫЛКИ ВОЗНИКНОВЕНИЯ КИБЕРУГРОЗ НА ОБЪЕКТЫ ТЭК В РФ

- Несоответствие технологического уровня российских организаций топливно-энергетического комплекса современным мировым требованиям
- Чрезмерная зависимость деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков
- Недостаточный уровень защищенности инфраструктуры и объектов топливно-энергетического комплекса от актов незаконного вмешательства

ITU: глобальный индекс кибербезопасности РФ в 2018 г. – 26 место из 194 стран, входящих в ООН

Кибербезопасность в энергетике

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ

187-ФЗ от 26.07.2017 «О безопасности КИИ РФ»

193-ФЗ от 26.07.2017 «О внесении изменений в …ФЗ о ГТ, о связи, о защите прав ЮЛ»

194-ФЗ от 26.07.2017 «О внесении изменений в УК и УПК РФ…»

127-ПП от 08.02.2018 «Об утверждении правил категорирования ОКИИ РФ…»

235-й приказ ФСТЭК от 21.12.2017 «Об утверждении Требований к созданию систем безопасности ЗОКИИ РФ»

239-й приказ ФСТЭК от 25.12.2017 «Об утверждении Требований по обеспечению безопасности ЗОКИИ РФ»

Приказы и методические документы ФСБ по ГосСОПКА (государственная система обнаружения и предотвращения компьютерных атак)

Кибербезопасность в энергетике

ЭТАПЫ ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ 187-ФЗ

01 Категорирование объектов КИИ – напрямую связано с идентификацией и оценкой рисков

02 Обеспечение безопасности значимых объектов КИИ

03 Присоединение к ГосСОПКА

Кибербезопасность в энергетике

КЛЮЧЕВЫЕ ЭТАПЫ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КИИ

Анализ угроз,
уязвимостей и нарушителей
в отношении объектов КИИ

Оценка возможных последствий
в случае возникновения
компьютерных инцидентов
(реализации **киберрисков**)

Определение категории значимости
для каждого объекта КИИ

Кибербезопасность в энергетике

ОЦЕНИВАНИЕ КИБЕРРИСКОВ

Причинение ущерба жизни и здоровью людей

Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации

Вредные воздействия на окружающую среду

Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения

Кибербезопасность в энергетике

СОЗДАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Обеспечение безопасности на всех этапах жизненного цикла:

- Создание/модернизация
- Эксплуатация
- Вывод из эксплуатации

Разработка, реализация и эксплуатация системы безопасности:

- Предотвращение неправомерного доступа к информации
- Недопущение воздействия на технические средства обработки информации
- Восстановление функционирования значимого объекта
- Непрерывное взаимодействие с ГосСОПКА

Кибербезопасность в энергетике

ВАРИАНТЫ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ К ГОССОПКА

СОЗДАТЬ СОБСТВЕННЫЙ ЦЕНТР

- Выполнить организационные и технические требования
- Обеспечить взаимодействие с НКЦКИ

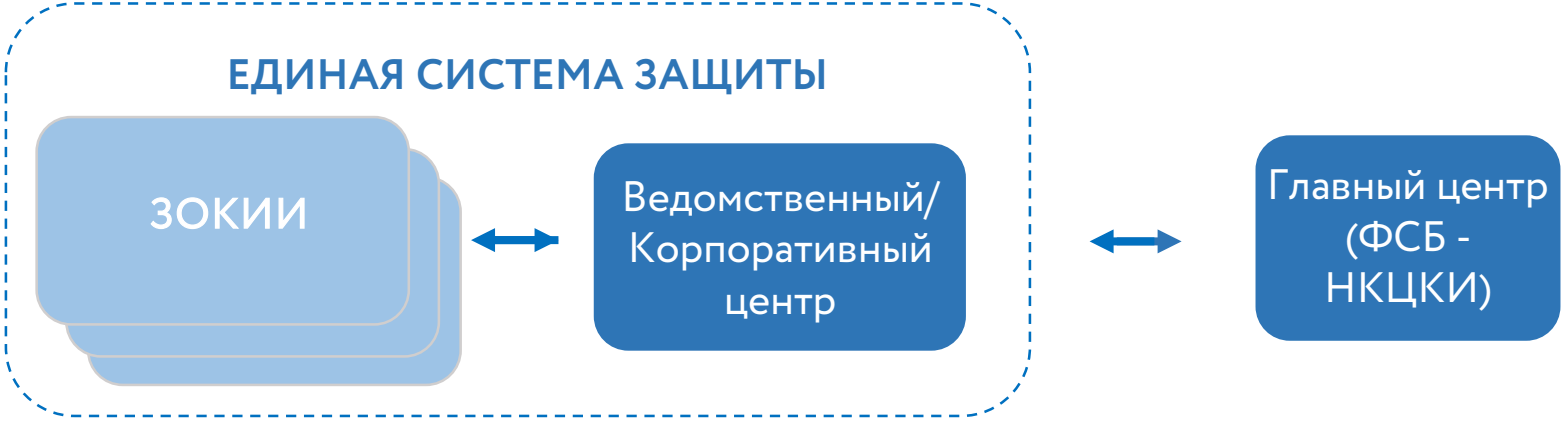
ИСПОЛЬЗОВАТЬ ВНЕШНИЙ ЦЕНТР

- Заключить соглашение с внешним центром
- Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности внешнего центра

Гибридный вариант: часть функций выполнять самостоятельно, часть – потреблять из внешнего центра

Кибербезопасность в энергетике

ВАРИАНТЫ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ К ГОССОПКА



Кибербезопасность в энергетике

ФУНКЦИИ ЦЕНТРОВ ГОССОПКА

- Инвентаризация информационных ресурсов
- Выявление уязвимостей информационных ресурсов
- Анализ угроз информационной безопасности
- Повышение квалификации персонала информационных ресурсов
- Прием сообщений о возможных инцидентах от персонала и пользователей информационных ресурсов
- Обеспечение процесса обнаружения компьютерных атак
- Анализ данных о событиях безопасности
- Регистрация инцидентов
- Реагирование на инциденты и ликвидация их последствий
- Установление причин инцидентов
- Анализ результатов устранения последствий инцидентов
- Взаимодействие с НКЦКИ

Кибербезопасность в энергетике

НЕОБХОДИМЫЕ СРЕДСТВА ДЛЯ ПОДКЛЮЧЕНИЯ К ГОССОПКА

ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК
средства мониторинга событий ИБ

ПРЕДУПРЕЖДЕНИЕ КОМПЬЮТЕРНЫХ АТАК
средства анализа защищенности

ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК
средства управления расследованием инцидентов и взаимодействия с ГосСОПКА

ПОИСК ПРИЗНАКОВ КОМПЬЮТЕРНЫХ АТАК
средства анализа и хранения копий сетевого трафика в сетях электросвязи

КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
должны быть сертифицированы

СРЕДСТВА ОБМЕНА ИНФОРМАЦИЕЙ
средства обеспечения передачи, приема и целостности информации в ходе работы средств ГосСОПКА

Кибербезопасность в энергетике

БЛИЖАЙШИЕ ПЕРСПЕКТИВЫ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ ТЭК В РФ

- Совершенствование и гармонизация законодательных и нормативных требований в области кибербезопасности объектов КИИ, включая область ТЭК
- Обеспечение субъектами КИИ соответствия требованиям 187-ФЗ
- Тренд на использование российских средств защиты информации при создании систем безопасности значимых объектов КИИ в ТЭК

Информино 2020

Москва, Россия
14-17 апреля 2020 г.

Спасибо за внимание!

Контакты докладчика:

Евгений Дружинин

КРОК

edruzhinin@croc.ru

www.croc.ru

IEEE

МОИ | Национальный исследовательский университет

КРОК