



ПРАКТИКА ПОСТРОЕНИЯ СОИБ

ПРОБЛЕМЫ | РЕШЕНИЯ | КЕЙСЫ

III вебинар цикла «Обеспечение безопасности объектов КИИ в рамках 187-ФЗ»



Проблемы ОКИИ в части ИБ

Недостаточно информации о текущем состоянии инфраструктуры



Нет данных о составе
компонентов



Нет данных по сетевому
обмену узлов сети

Проблемы АСУ ТП в части ИБ

Неготовность инфраструктуры и сети к наложению СРЗИ



Устаревшее ПО



Слабое аппаратное
обеспечение



Отсутствие технических
условий

Проблемы ОКИИ в части ИБ

Неготовность инфраструктуры и сети к наложению СРЗИ



Не предъявлялись
требования к ИБ на этапе
проектирования



Проблемы с выделением
бюджета на подсистему ИБ



Стремление построить ИБ
исключительно на бумаге

Проблемы сетевой инфраструктуры в части ИБ



Различные типы
оборудования



Уход вендоров



Нет системного подхода по
построению сети

Предпосылки к внедрению СОИБ

Вызовы окружающей действительности



Рост количества
целевых атак



Доступность средств
их осуществления





Необходимость
в периодической работе
сотрудников сторонних
организации





Низкая вовлеченность
сотрудников в процесс
осуществления ИБ


Предпосылки к внедрению СОИБ

-  **Федеральный закон № 149-ФЗ от 27.07.2006 г.**
«Об информации, информационных технологиях и о защите информации»

-  **Приказ ФСТЭК России № 31 от 14.03.2014 г.**
«Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

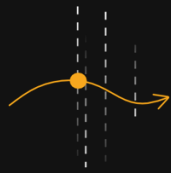
-  **Федеральный закон от № 187-ФЗ от 26.07.2017 г.**
«О безопасности критической информационной инфраструктуры Российской Федерации»

-  **Приказ ФСТЭК России № 235 от 21.12.2017 г.**
«Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

-  **Приказ ФСТЭК России № 239 от 25.12.2017 г.**
«Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Предпосылки к внедрению СОИБ

Внедрение систем интеграции АСУ



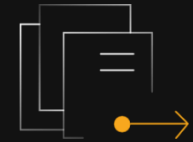
Учет ресурсов



Сбор данных



Диспетчеризация



Отправка данных
в корпоративные
системы

Что СОИБ предложит каждому из вас



ПРОИЗВОДСТВО

повышение
осведомленности



СЛУЖБА ИБ

автоматизация
работы



РУКОВОДСТВО

отсутствие штрафов
и простоев

СОИБ развиваются



От точечных внедрений
к комплексным системам



Импортозамещение
в действии



Расширение
функционала

Текущий состав типовых проектов

- Антивирусная защита
- Резервное копирование и восстановление
- Межсетевое экранирование
- Система обнаружения вторжений
- Управление доступом
- Обнаружение и анализ уязвимостей
- Контроль целостности
- Средство анализа событий информационной безопасности
- Управление СОИБ

Масштабирование систем. С чего начать?

00.

Выделение функциональных ролей и разработка ОРД

01.

Анализ исходных данных:
сеть и защита конечных точек

02.

Приведение в порядок инфраструктуры:
проверить действующие настройки

03.

Расширение состава средств

04.

Развитие существующих систем

КЕЙС #1 Энергокомпания

ЗАКАЗЧИК

ЭНЕРГОКОМПАНИЯ

ОСОБЕННОСТИ

1. Распределенная административная и географическая структура (изолированные ГРЭС)
2. Большое количество типов систем АСУ ТП
3. Возможность работ только в период технических остановок
4. В процессе ПНР появилось требование Заказчика по подключению СОИБ к коммерческому SOC

РЕЗУЛЬТАТ

1. Проведено проектирование и внедрение комплексной СОИБ на всех станциях
2. Проведено подключение к коммерческому SOC
3. Осуществляется техническая поддержка внедренных решений

КЕЙС #1 Энергокомпания

Внедренные сервисы

3

площадки

310

АРМ

144

сервера

295

АСО

83

ОКИИ

1. Сетевые сервисы — МЭ, IPS+IDS на платформе Fortinet
2. Сервисы РК — решение на базе ПО Кибер Бэкап + СХД
3. Сервисы виртуализации — инфраструктура и виртуальные рабочие места
4. Сервисы АВЗ — ПО KES + KICS
5. Сервисы службы каталога — аутентификация и контроль доступа
6. Сервисы PKI — реализация усиленной аутентификацией
7. Сервисы обновлений — реализация центра обновления ПО
8. Сервисы СКДПУ — реализация контроля привилегированных пользователей
9. Сервисы анализа и мониторинга состояний ИБ

КЕЙС #2 Энергокомпания

ЗАКАЗЧИК

ЭНЕРГОКОМПАНИЯ

ОСОБЕННОСТИ

1. Распределенная административная и географическая структура (изолированные ГРЭС)
2. Системы АСУ ТП разных типов
3. Необходимость разделения сетей АСУ ТП и КСПД
4. Возможность работ только в период технических остановок

РЕЗУЛЬТАТ

1. Проведены работы по сегментации сети
2. Проведено проектирование и внедрение комплексной СОИБ на всех станциях
3. Ведется регулярное сопровождение (аудит и устранение уязвимостей)

КЕЙС #2 Энергокомпания

Внедренные сервисы

1. Сервисы АВЗ
2. Сетевые сервисы
3. Сервисы средств анализа и мониторинга состояния ИБ
4. Сервисы резервного копирования и восстановления

Немного цифр

1342
ОЗ

131
ПТК

31
ЗОКИИ

31
вендора АСУ

КЕЙС #3 Metallurgical holding

ЗАКАЗЧИК **МЕТАЛЛУРГИЧЕСКИЙ ХОЛДИНГ**

ОСОБЕННОСТИ

1. Системы АСУ ТП разного назначения
2. Необходимость проведения сегментирования сетей
3. Совместная работа по созданию внутреннего SOC

РЕЗУЛЬТАТ

1. Успешно проведена разработка и внедрения СОИБ
2. Производится масштабирование системы на площадках дочерних компании
3. Осуществляется техническая поддержка внедренных решений

КЕЙС #4 Нефтегазовая компания

ЗАКАЗЧИК

НЕФТЕГАЗОВАЯ КОМПАНИЯ

ОСОБЕННОСТИ

1. Широкая география
2. Требования по использованию УТР
3. Необходимость сопровождения аттестации ФСТЭК внедренных решений

РЕЗУЛЬТАТ

1. Успешное построение СОИБ в несколько этапов
2. Производится масштабирование системы в строящихся очередях СОИБ
3. Осуществляется техническая поддержка внедренных решений

КЕЙС #5 Энергокомпания

ЗАКАЗЧИК

ЭНЕРГОКОМПАНИЯ

ОСОБЕННОСТИ

1. Распределенная административная и географическая структура (ТЭЦ)
2. Системы АСУ ТП разных типов
3. Необходимость разделения сетей АСУ ТП и КСПД
4. Возможность проведения работ только в период технических остановок

РЕЗУЛЬТАТ

1. Успешно проведена разработка и внедрения СОИБ
2. Производится масштабирование системы на площадках дочерних компании
3. Осуществляется техническая поддержка внедренных решений

КЕЙС #6 Газовая компания

ЗАКАЗЧИК

ГАЗОВАЯ КОМПАНИЯ

ОСОБЕННОСТИ

1. Проектирование СОИБ на строящихся АСУ
2. Системы АСУ ТП разных типов
3. Необходимость согласования настроек с большим количеством участников

РЕЗУЛЬТАТ

1. Успешно проведена разработка и внедрение СОИБ
2. Осуществляется техническая поддержка внедренных решений
3. Прорабатываются варианты импортозамещения СрЗИ

Выводы



Типовые проблемы
решаемы. Есть опыт



Важен **индивидуальный
подход** к каждому кейсу



Работы предстоит
МНОГО

Уральский центр систем безопасности (УЦСБ)

> 16

лет на рынке

> 1000

профессионалов в штате

> 2000

реализованных проектов

Топ-100 крупнейших отечественных ИТ-компаний ¹

Топ-15 крупнейших компаний России в сфере защиты информации ²

Компетенции

- Информационная безопасность
- Информационные технологии
- Инженерно-технические средства охраны
- Анализ защищенности
- Центры обработки данных
- Умный дом
- Сервисный центр

¹ Рейтинг CNews100: Крупнейшие ИТ-компании России 2023

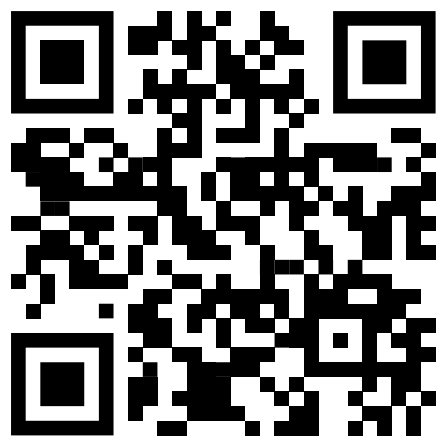
² Рейтинг CNews Security: Крупнейшие компании России в сфере защиты информации 2023

ПРОГРАММА ВЕБИНАРОВ

- 19.03** ■ Как защитить КИИ от киберугроз? (Категорирование КИИ)
- 09.04** ■ Как построить эффективную систему обеспечения ИБ объектов КИИ
- 25.04** ■ Практические кейсы построения СОИБ
- 21.05** ■ Мониторинг ЗОКИИ (SOC)
 - Безопасная разработка ПО для значимых объектов КИИ
 - Оценка защищенности для ЗОКИИ (с учетом Указа Президента РФ № 250)
 - Подготовка к прохождению госконтроля

Подписывайтесь на наш канал в Телеграме

- Ежемесячные обзоры изменения законодательства
- Разбор часто задаваемых вопросов по теме КИИ
- Экспертные статьи и кейсы





СПАСИБО ЗА ВНИМАНИЕ! ВОПРОСЫ?

Александр Мерзляков

Руководитель группы внедрения
и поддержки специального ПО

2024

compliance@ussc.ru

www.ussc.ru

