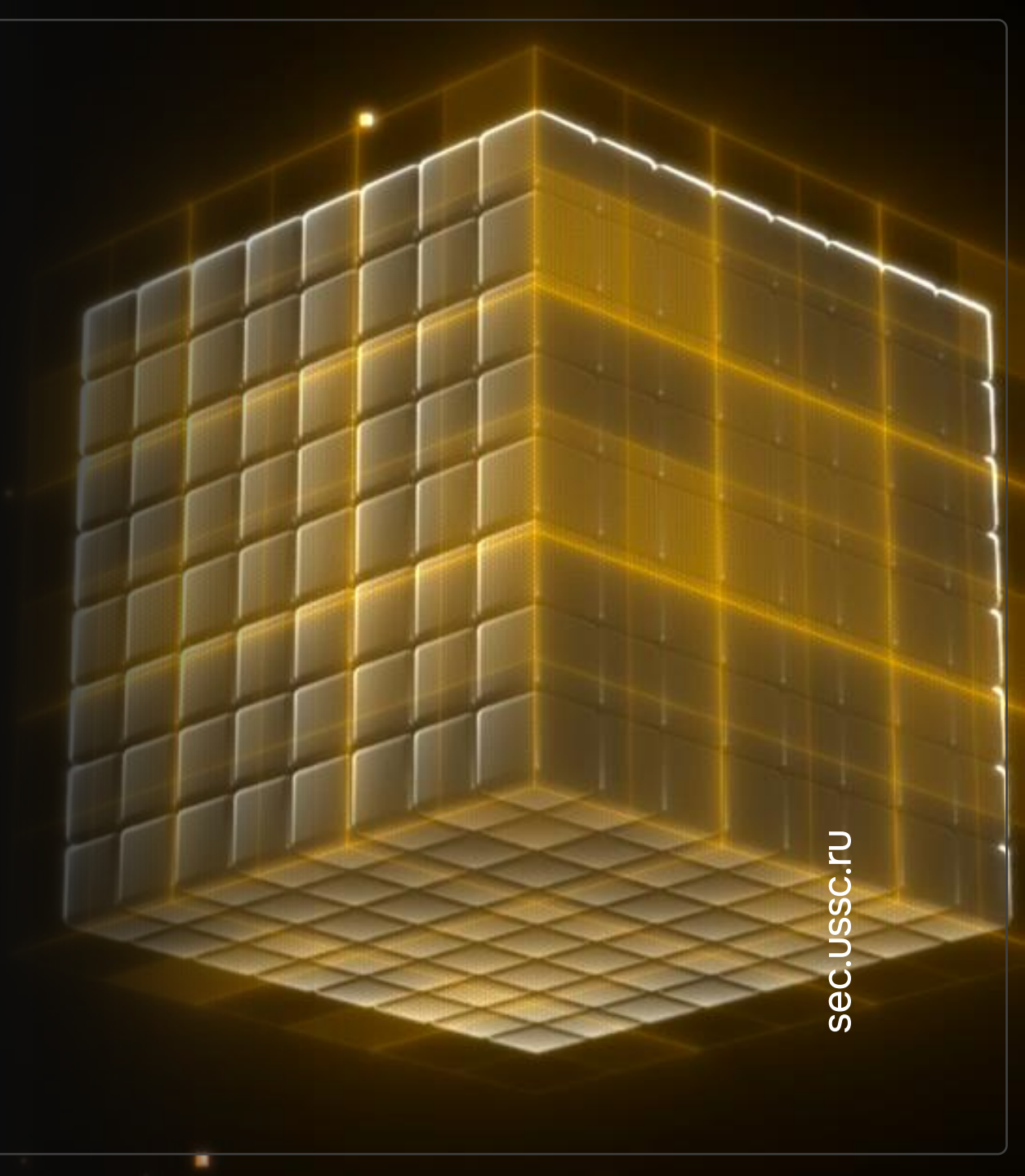
ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

Обеспечение ИБ АСУ ТП на практике

Александр Мерзляков
Руководитель группы внедрения
и поддержки специального ПО



sec.ussc.ru

01. Проблемы АСУ ТП в части ИБ

Раздел ИБ не предусмотрен проектом АСУ

АСУ ТП проектировалось как изолированная

!

Не предъявлялись требования к ИБ на этапе проектирования

!

02. Проблемы АСУ ТП в части ИБ

Недостаточно информации о текущем состоянии инфраструктуры

!

Нет данных о составе компонентов сети АСУ ТП

!

Нет данных по сетевому обмену узлов сети

03. Проблемы АСУ ТП в части ИБ

Неготовность инфраструктуры и сети к наложению СРЗИ

- Устаревшее ПО !
- Слабое аппаратное обеспечение !
- Отсутствие технических условий !

04. Предпосылки к внедрению СОИБ

Внедрение систем интеграции АСУ

Учет ресурсов

Сбор данных

Диспетчеризация

Отправка данных
в корпоративные системы

05. Предпосылки к внедрению СОИБ

Вызовы окружающей действительности

Рост количества целевых атак

Доступность средств их осуществления

Необходимость в периодической работе на оборудовании АСУ ТП сотрудников сторонних организации

Низкая вовлеченность сотрудников в процесс осуществления ИБ

06. 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»

07. Что СОИБ предложит каждому из вас

ПРОИЗВОДСТВО

повышение осведомленности

СЛУЖБА ИБ

автоматизация работы

РУКОВОДСТВО

отсутствие штрафов и простоев

08. СОИБ развиваются

От точечных внедрений
к комплексным системам

Импортозамещение
в действии

Расширение
функционала

09. 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

10. Масштабирование систем. С чего начать?

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

11. 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

12. 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 остановов

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)

13. КЕЙС #3 Металлургический холдинг

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

14. Выводы

Типовые проблемы решаемы. Есть опыт

Важен индивидуальный подход к каждому кейсу

Работы предстоит много

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Александр Мерзляков
Руководитель группы внедрения
и поддержки специального ПО

amerzlyakov@ussc.ru +7 (953) 824-45-75