



Кибербезопасность объектов КИИ: насущные проблемы и пути их решения



Спикер:

- Егорова Татьяна – заместитель руководителя департамента интеграционных решений по вопросам промышленной кибербезопасности, КСБ-СОФТ

«КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

70+

регионов внедрения

4000+

реализованных проектов

НАШИ УСЛУГИ



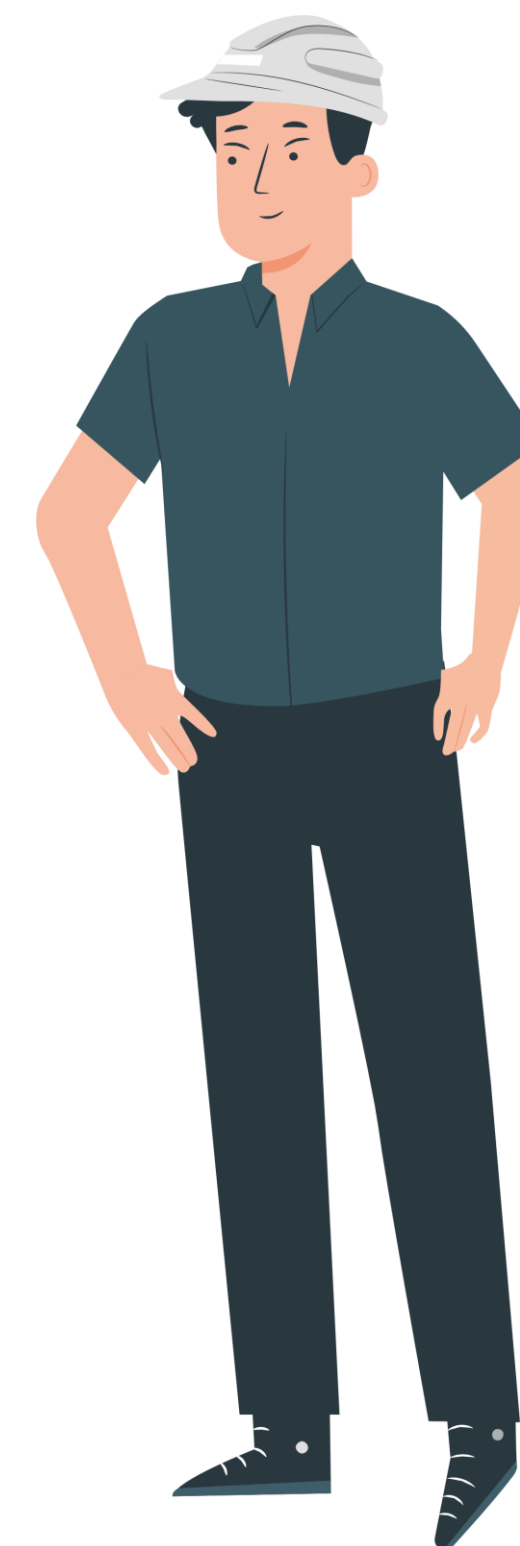
КАК МЫ РАБОТАЕМ

1 ЭТАП. ФОРМИРУЕМ ТРЕБОВАНИЯ К ЗАЩИТЕ

- Предпроектное обследование АСУ ТП
- Классификация АСУ ТП по требованиям защиты информации
- Разработка модели угроз безопасности
- Анализ уязвимостей АСУ ТП с формированием рекомендаций по их закрытию
- Разработка технического задания на создание системы защиты

2 ЭТАП. РАЗРАБАТЫВАЕМ СИСТЕМУ ЗАЩИТЫ

- Проектирование системы защиты
- Стендовые испытания проектных решений
- Разработка эксплуатационной и рабочей документации
- Рекомендации по настройке основного и прикладного ПО в АСУ ТП



КАК МЫ РАБОТАЕМ

3 ЭТАП. ВНЕДРЯЕМ СИСТЕМУ ЗАЩИТЫ АСУ ТП И ВВОДИМ ЕЕ В ЭКСПЛУАТАЦИЮ

- Поставка средств защиты
- Внедрение поставленных средств
- Разработка организационно-распорядительной документации
- Испытания системы защиты (предварительные, приемочные, аттестационные)

4 ЭТАП. СОПРОВОЖДАЕМ СИСТЕМУ ЗАЩИТЫ АСУ ТП В ХОДЕ ЕЕ ЭКСПЛУАТАЦИИ

- Мониторинг эффективности принимаемых мер по защите информации
- Помощь в расследовании инцидентов безопасности



ПОРТФОЛИО В ЧАСТИ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ ЗА 2023 Г.

Сфера: энергетика.

Конечный Заказчик: ПАО «Россети» и его филиалы.

Объекты защиты: АСУ ТП электрических подстанций 500 кВ, 330 кВ, 220 кВ

Работы: проектирование СИБ, пусконаладочные работы СИБ

Сфера: топливно-энергетический комплекс.

Конечный Заказчик: ООО «Арктик СПГ 2», АО «Верхнечонскнефтегаз» (ПАО «НК «Роснефть»)

Объекты защиты: АСУ по управлению электроснабжением, пожарной сигнализации и управления пожаротушением

Работы: проектирование СИБ, пусконаладочные работы СИБ

Сфера: транспорт.

Конечный Заказчик: ФГБУ «Канал имени Москвы»

Объекты защиты: АСУ телемеханики, контроля шлюзования, судопропуска и т.д.

Работы: проектирование СИБ

НАСУЩНЫЕ ПРОБЛЕМЫ

ОТСУТСТВИЕ ОСОЗНАННОГО ПОДХОДА ПО СОЗДАНИЮ СОИБ ОКИИ

- Подходы и способы реализации СОИБ имеют разнородный характер даже в рамках одного холдинга, группы компаний
- К подрядчикам не предъявляются требования по ИБ
- Не проводится обучение персонала правилам ИБ
- Сложности с мониторингом событий ИБ в изолированных АСУ ТП
- Организационные меры разрабатываются не в полном объеме
- Мероприятия, прописанные в ОРД, не выполняются
- Нехватка специалистов ИБ

РАЗДЕЛ ИБ ПО «ОСТАТОЧНОМУ ПРИНЦИПУ»



Отсутствие проектного подхода к созданию системы ИБ



Проблемы с выделением бюджета на работы по ИБ



При проектировании АСУ ТП Заказчики забывают заложить требования по ИБ



Не выстроены процессы по ИБ



СОИБ не закладывается на стадии проектирования АСУ ТП, в результате чего СЗИ внедряются уже в рамках функционирования АСУ ТП



Долгое согласование заявок на проведение работ

КОММУНИКАЦИИ ВНУТРИ СУБЪЕКТОВ КИИ



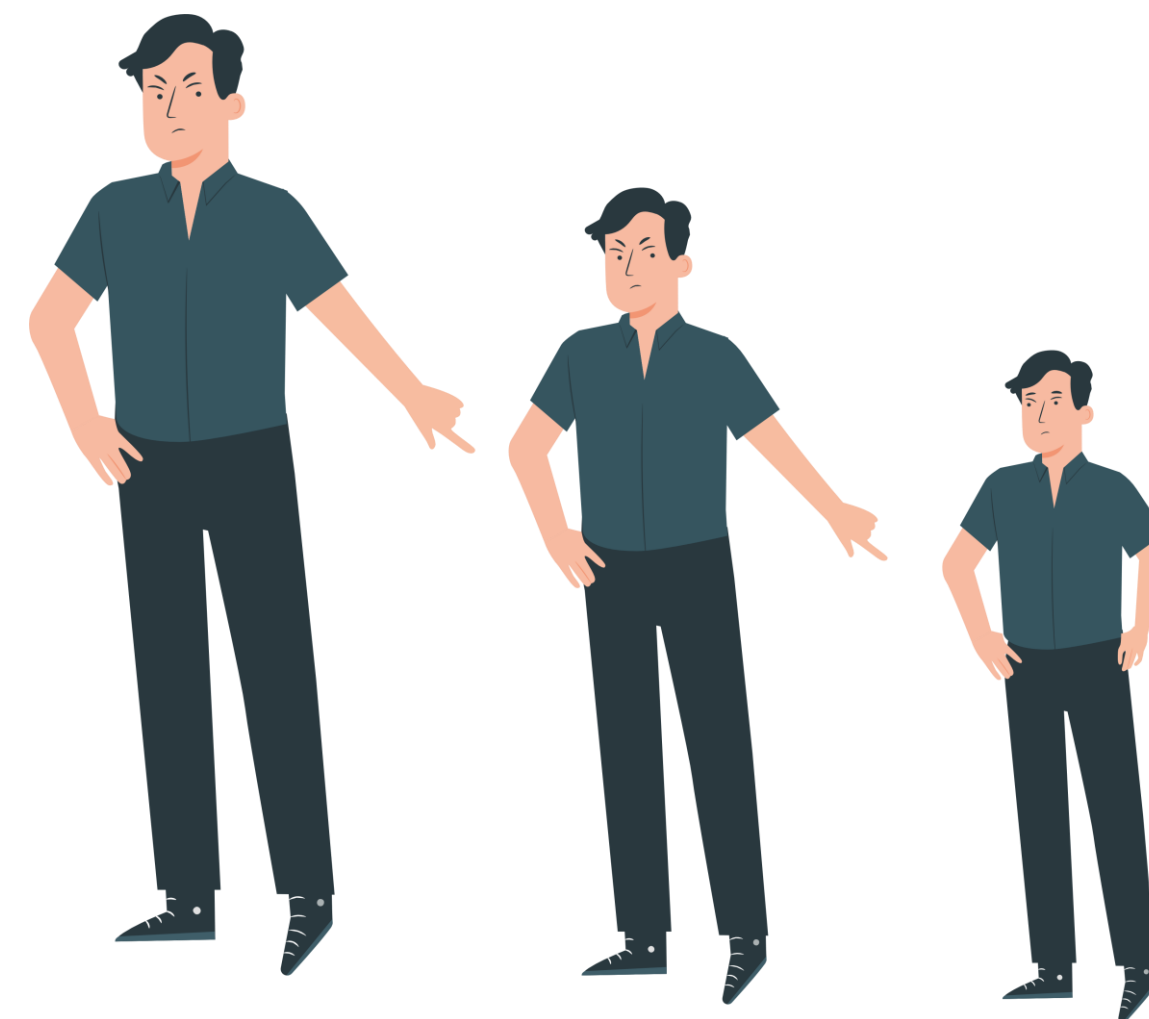
Недостаточное взаимодействие специалистов из разных служб/отделов (АСУ, связь, ИБ и т.д.)



Перекладывание ответственности



Низкая осведомленность персонала в вопросах ИБ



СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ



На рынке мало СЗИ
в промышленном
исполнении



СЗИ должным образом
не пилотируются перед
внедрением



Перегруженная техподдержка
производителей



Политика лицензирования
СЗИ без учета специфики сферы

ИМПОРТОЗАМЕЩЕНИЕ



Отсутствие отечественных аналогов ПО и оборудования для АСУ ТП



Большинство АСУ ТП продолжает работать на уязвимых версиях ОС



Устаревшее ПО и оборудование АСУ ТП не совместимы с современными СЗИ

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА В ЧАСТИ КИИ



Седьмой год продолжаются бесконечные споры в части выделения ОКИИ, подлежащих категорированию и определения критических процессов



Субъекты КИИ стремятся уйти от категории значимости ОКИИ



В некоторых отраслях недавно опубликованные типовые перечни ОКИИ вызывают вопросы у субъектов КИИ



Отсутствует методический документ по выполнению требований 239 приказа ФСТЭК России



Обеспечение полноценного мониторинга ИБ и подключение к ГосСОПКА откладывается в долгий ящик



В НПА отсутствуют требования к подрядчикам в сфере КИИ

ПУТИ РЕШЕНИЯ

СО СТОРОНЫ СУБЪЕКТОВ КИИ:

- 1) Формирование осознанности первых лиц и персонала субъектов КИИ в части важности обеспечения ИБ
- 2) Выстраивание процессов внутри субъектов КИИ, прозрачное распределение ответственности
- 3) Регулярное обучение персонала правилам безопасной работы

СО СТОРОНЫ ВЕНДОРОВ, ИНТЕГРАТОРОВ:

- 1) Более внимательное отношение к особенностям сферы
- 2) Оперативная и качественная техподдержка интеграторов
- 3) Постоянный обмен опытом, организация практических бесплатных вебинаров с разборами кейсов в части ИБ

СО СТОРОНЫ РЕГУЛЯТОРОВ:

- 1) Методические документы и публичные мероприятия по разъяснению требований НПА
- 2) Упрощение/ускорение процедуры сертификации СЗИ
- 3) Закрепление в НПА требований к подрядчикам в сфере КИИ

Услуги КСБ-СОФТ

Компания КСБ-СОФТ оказывает полный комплекс услуг по защите объектов КИИ

Мы поможем Вам защитить данные и выполнить требования НПА



Безопасность объектов КИИ

Выявление и категорирование объектов КИИ, разработка и внедрение комплексного решения по обеспечению безопасности значимых объектов КИИ, организация взаимодействия с центром ГосСОПКА, анализ уязвимостей и пентест



Импортозамещение

Решение задач импортозамещения в соответствии со стратегией развития информационного общества в Российской Федерации



SOCRAT - центр мониторинга и реагирования на инциденты информационной безопасности

Мониторинг и предотвращение атак на начальных стадиях, либо выявление следов проникновения

<https://rutube.ru/video/8048df2267bf671cd042799a7da6a088/?r=wd>

ПК АльфаДок. Автоматизация процессов по защите информации



- Разработка и актуализация документации, журналов
- Учет защищаемых ресурсов и средств защиты информации
- Моделирование угроз безопасности и определение мер по защите информации
- Оценка защищенности систем, анализ уязвимостей
- Категорирование объектов КИИ с разработкой документации в соответствии с приказом ФСТЭК России № 239
- Планирование деятельности, оценка готовности к проверкам
- Учет и реагирование на инциденты информационной безопасности

Работайте с нами!



<https://ksb-soft.ru/>



428000, г. Чебоксары,
пр-т Максима Горького,
18 Б, пом. 9



8 800 3333-872



info@ksb-soft.ru



Телеграм-канал
«Мнение интегратора»

