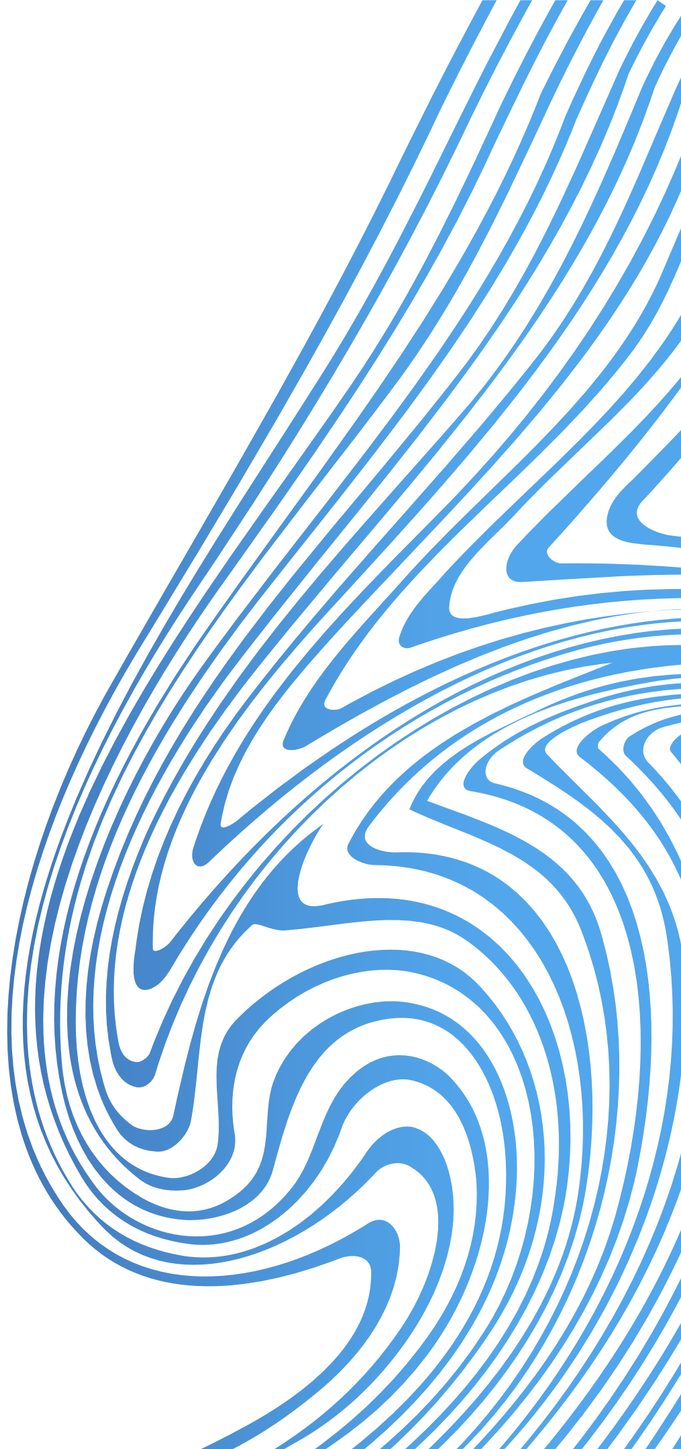
КСБ-СОФТ

БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ (АСУ ТП)



КИБЕРРЕАЛИИ АСУ ТП

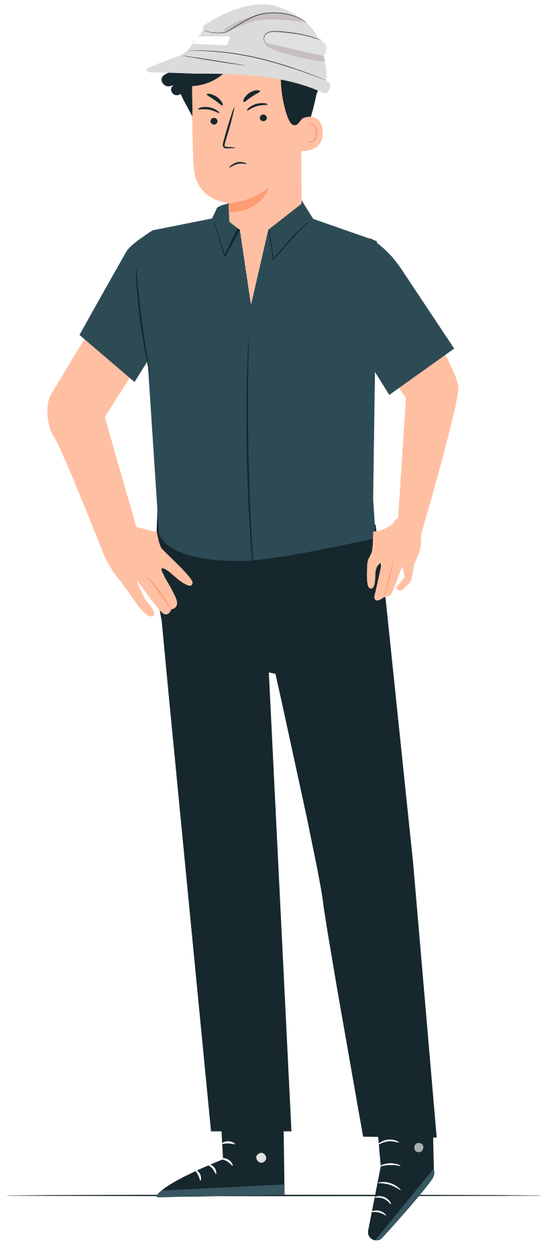
01 Сложные целенаправленные атаки на инфраструктуру промышленных организаций – бич прошлого года

02 Количество кибератак в 2023 году выросло в 1,7 раз

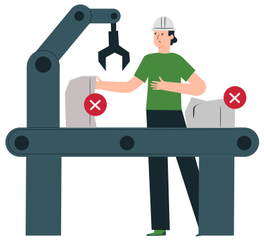
03 Эксплуатация уязвимостей – один из самых частых сценариев проникновения в инфраструктуру

04 Каждая 10-я организация не признает факт взлома, даже после обнародования доказательств

05 Февраль, апрель, июнь – самые «богатые» на взлом месяцы 2023 года



САМЫЕ ЧАСТЫЕ ПОСЛЕДСТВИЯ АТАК НА ПРОМЫШЛЕННЫЕ ОРГАНИЗАЦИИ



Остановка производства

Перебой в работе автоматизированных систем

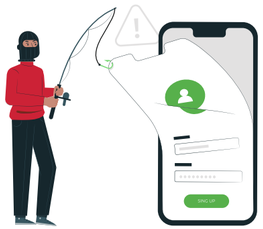
Прямые убытки

Штрафы

Прекращение отгрузки продукции

Шантаж и вымогательство

Утечки ПДн



Кража конфиденциальной информации

Уголовная ответственность за нарушение требований законодательства

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ ТП

Технологические особенности

Применение средств защиты в АСУ ТП имеет ограничение – они не должны влиять на технологический процесс

Промышленные организации не способны закрывать уязвимости в короткие сроки

Для обслуживания АСУ ТП привлекается много подрядных организаций

Отдельные элементы АСУ ТП часто располагаются за пределами контролируемой зоны

Каналы передачи информации в АСУ ТП слабо защищены

Срок службы промышленного оборудования и ПО гораздо больше, чем у информационных технологий в АСУ ТП

Нет системного подхода к построению системы защиты АСУ ТП

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ ТП

Законодательные требования

Много требований к защите АСУ ТП и КИИ*

Часто меняющиеся требования

№ 187-ФЗ
о безопасности КИИ

Указ Президента РФ №250
о дополнительных мерах обеспечения ИБ

Приказ ФСТЭК № 239
о требованиях к защите объектов КИИ

Приказ ФСТЭК № 31
о требованиях к защите информации в АСУ ТП

Приказ ФСТЭК № 235
о требованиях к созданию систем безопасности ЗОКИИ

Отраслевые требования
по информационной безопасности

*Критическая информационная инфраструктура

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ ТП

Причины возникновения угроз

Недостаточная осведомленность сотрудников в вопросах кибергигиены

Высокий уровень компетенций злоумышленников

Ежедневное появление новых уязвимостей в ПО

Наличие на просторах интернета готовых сценариев эксплуатации уязвимостей

Высокий уровень автоматизации

Сложность и разнообразие инфраструктуры промышленных предприятий

Мнимое чувство защищенности изолированных сетей АСУ ТП

НАШЕ РЕШЕНИЕ

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

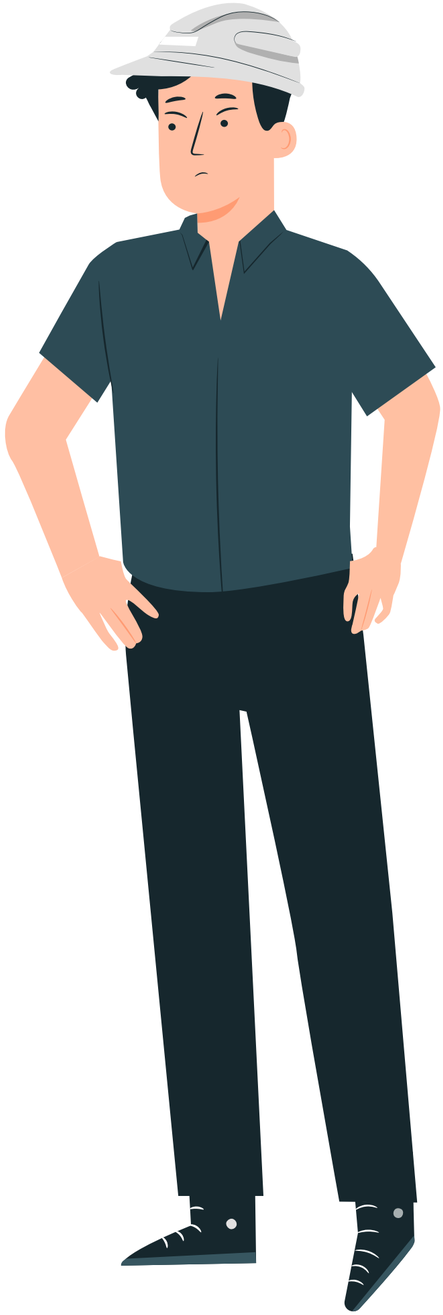
2 ЭТАП.
Разрабатываем систему защиты

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 (предварительные, приемочные, аттестационные) системы защиты

4 ЭТАП.
Сопровождаем систему защиты АСУ ТП в ходе ее эксплуатации

Мониторинг эффективности принимаемых мер по защите информации

Помощь в расследовании инцидентов безопасности

БЕЗОПАСНОСТЬ АСУ ТП С КОМАНДОЙ ИНЖЕНЕРОВ КСБ-СОФТ – ЭТО

Реальная защищенность информации в АСУ ТП

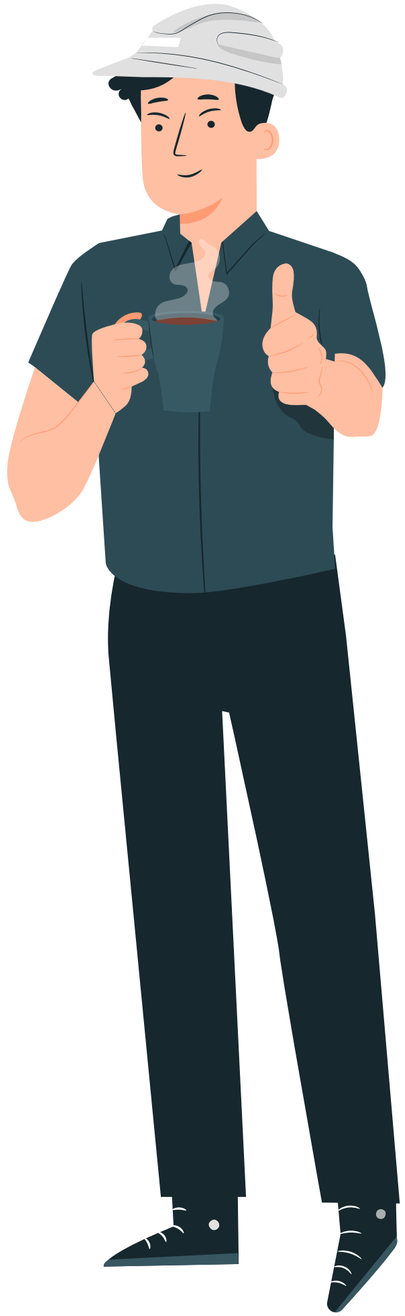
Обеспечение информационной безопасности на всех этапах работ

Выполнение законодательных требований

Устойчивое функционирование АСУ ТП

Полный комплект документации на систему защиты АСУ ТП

Обеспечение совместимости средств защиты и АСУ ТП



КОМПАНИЯ КСБ-СОФТ

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

Обеспечение безопасности КИИ и АСУ ТП

Мониторинг и реагирование на инциденты ИБ

Консалтинг по безопасной разработке и сертификации СЗИ

Анализ уязвимостей и тестирование на проникновение

Аудит информационной безопасности

Защита информации в ГИС и ИСПДн

Наш вклад в кибербезопасность

Защита значимых объектов КИИ РФ

Разработанные командой КСБ-СОФТ специализированные утилиты и скрипты для тестирования безопасности ИТ-инфраструктуры организаций

Созданный в соответствии с передовыми практиками цикл безопасной разработки

Активная деятельность в российском комьюнити безопасной разработки

Наши клиенты – государственные и коммерческие организации в 80 регионах России

На сегодня в портфолио компании более 4000 проектов разной степени сложности, полученный опыт в которых помогает нам подбирать эффективные решения для защиты информационных ресурсов наших клиентов

КСБ-СОФТ

8 800 3333-872

+7 (8352) 322-322

info@ksb-soft.ru

КАНАЛ
«МНЕНИЕ ИНТЕГРАТОРА»

ПОДКАСТ
«SOCRAT ЗА СТЕКЛОМ»

САЙТ
КОМПАНИИ