КСБ-СОФТ

БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ (АСУ ТП)

КИБЕРРЕАЛИИ АСУ ТП

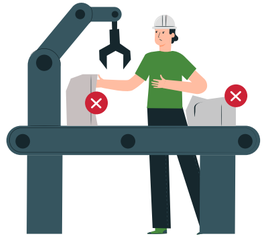
01 Ежегодное увеличение количества сложных целенаправленных атак на технологический сегмент промышленных предприятий

02 Атаки приводят к нарушению основной деятельности предприятий, шифрованию и утечкам конфиденциальной информации

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

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

САМЫЕ ЧАСТЫЕ ПОСЛЕДСТВИЯ АТАК НА ПРОМЫШЛЕННЫЕ ОРГАНИЗАЦИИ



Остановка производства

Перебой в работе автоматизированных систем

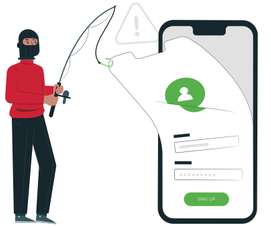
Прямые убытки

Утечки ПДн

Прекращение отгрузки продукции

Шантаж и вымогательство

Штрафы и уголовная ответственность за нарушение законо-дательных требований



Кража конфиденциальной информации

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ ТП

ТЕХНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ

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

02 Промышленные организации не способны закрывать уязвимости в короткие сроки

03 Для обслуживания АСУ ТП привлекается много подрядных организаций

04 Отдельные элементы АСУ ТП часто располагаются за пределами контролируемой зоны

05 Каналы передачи информации в АСУ ТП слабо защищены

06 Нет системного подхода к построению системы защиты АСУ ТП

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ ТП

ЗАКОНОДАТЕЛЬНЫЕ ТРЕБОВАНИЯ

Много часто меняющихся требований к защите АСУ ТП и КИИ*

№ 187-ФЗ о безопасности КИИ

Приказ ФСТЭК № 239
о требованиях
к защите объектов КИИ

Приказ ФСТЭК № 235
о требованиях к созданию
систем безопасности ЗОКИИ

Указ Президента РФ № 250
о дополнительных мерах
обеспечения ИБ

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

Отраслевые требования
по информационной
безопасности

Требования
по импортозамещению
(Указы 166, 250,
ПП РФ 1912 и т.д.)

*Критическая информационная инфраструктура

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУ ТП

ПРИЧИНЫ ВОЗНИКНОВЕНИЯ УГРОЗ

Недостаточная осведомленность сотрудников в вопросах кибергигиены

Высокий уровень автоматизации

Высокий уровень компетенций злоумышленников

Сложность и разнообразие инфраструктуры промышленных предприятий

Ежедневное появление новых уязвимостей в ПО

Мнимое чувство защищенности изолированных сетей АСУ ТП

Наличие на просторах интернета готовых сценариев эксплуатации уязвимостей

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 системы защиты (предварительные, приемочные, аттестационные)

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

- Мониторинг событий безопасности и 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

ОПЫТ КСБ-СОФТ

Ознакомиться с реальными кейсами можно в нашем портфолио – https://ksb-soft.ru/all-projects/

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 6000 проектов разной степени сложности, полученный опыт в которых помогает нам подбирать эффективные решения для защиты информационных ресурсов наших клиентов

КСБ-СОФТ

КОНТАКТЫ

8 800 3333-872
info@ksb-soft.ru
ksb-soft.ru