КСБ-СОФТ

Кибербезопасность объектов КИИ: насущные проблемы и пути их решения

Спикеры:

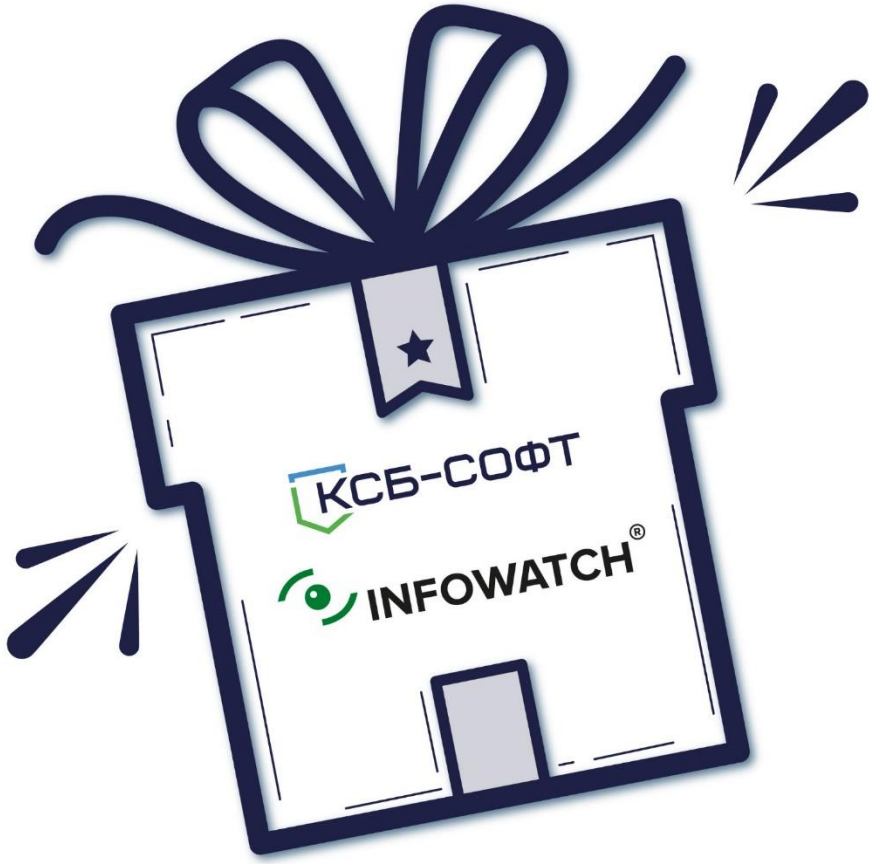
- Александр Ильин - руководитель регионального направления КСБ-СОФТ;
- Татьяна Егорова – заместитель руководителя департамента интеграционных решений по вопросам промышленной кибербезопасности, КСБ-СОФТ;
- Алексей Петухов - руководитель отдела развития продуктов InfoWatch.

Время проведения вебинара ~1 час

Обменивайтесь сообщениями
во вкладке «Чат»

Запись вебинара направим всем
участникам на указанный
при регистрации e-mail
в течение 2-3 рабочих дней

Задавайте вопросы во вкладке
«Вопросы»



Среди заданных вами вопросов, каждый Эксперт выберет лучший, на его взгляд, вопрос, и мы наградим 3-х авторов фирменным мерчем!

КСБ-СОФТ

Системный интегратор
в сфере информационной
безопасности и импортозамещения
информационных технологий

Входим в ГК «Кейсистемс»

Лицензиат ФСТЭК России

Лицензиат ФСБ России

Проекты компании курируют опытные ИБ-специалисты, аккредитованные по международным сертификациям OSCP, CISM, CGEIT и CISA.

80+
регионов внедрения

4000+
реализованных проектов

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

1 **Домен «Непрерывная безопасность. SOCRAT»**

Услуги центра мониторинга SOCRAT

Тестирование на проникновение (Pentest)

Анализ уязвимостей

Защита порталов (WAF)

Внедрение SIEM

2 **Домен «Промышленность. Субъекты КИИ»**

Безопасность объектов КИИ

Безопасность АСУ ТП

3 **Домен «Безопасная разработка»**

Аудит безопасности ПО

Внедрение процессов безопасной разработки (SDL)

Сертификация продуктов

4 **Домен «Органы власти. ГИС»**

Защита информации в ГИС

Обеспечение жизненного цикла ГИС (676 ПП)

Инвентаризация ГИС и контроль подключения (Экосистема Альфа)

5 **Домен «Коммерция. Защита ПДн и коммерческой тайны»**

Защита персональных данных

Защита коммерческой тайны

Защита от утечек информации (DLP)

6 **Домен «ИТ-интеграция»**

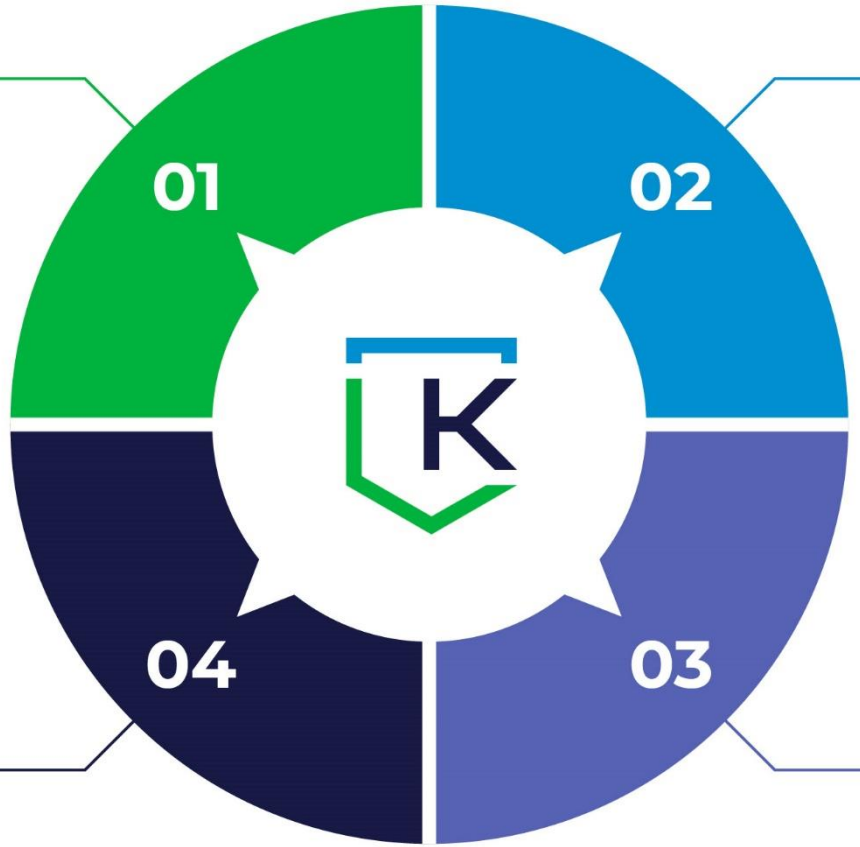
Импортозамещение

Внедрение ИТ-продуктов

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АСУ ТП

Формирование требований к системе защиты

Разработка системы защиты



Сопровождение системы защиты при ее эксплуатации

Поставка и внедрение системы защиты

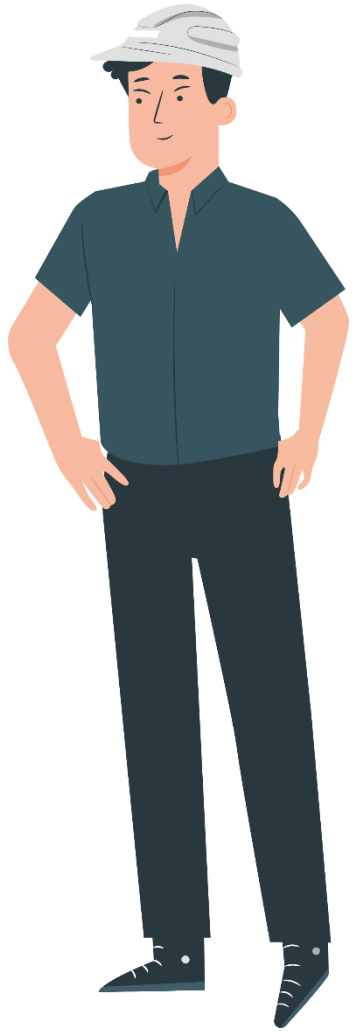
КАК МЫ РАБОТАЕМ

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

- Раздел ИБ по «остаточном принципу»

- Коммуникации внутри субъектов КИИ

- Средства защиты информации

- Импортозамещение

ОТСУТСТВИЕ ОСОЗНАННОГО ПОДХОДА ПО СОЗДАНИЮ СОИБ ОКИИ

Подходы и способы реализации СОИБ имеют разнородный характер даже в рамках одного холдинга, группы компаний

Организационные меры разрабатываются не в полном объеме

К подрядчикам не предъявляются требования по ИБ

Мероприятия, прописанные в ОРД, не выполняются

Не проводится обучение персонала правилам ИБ

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

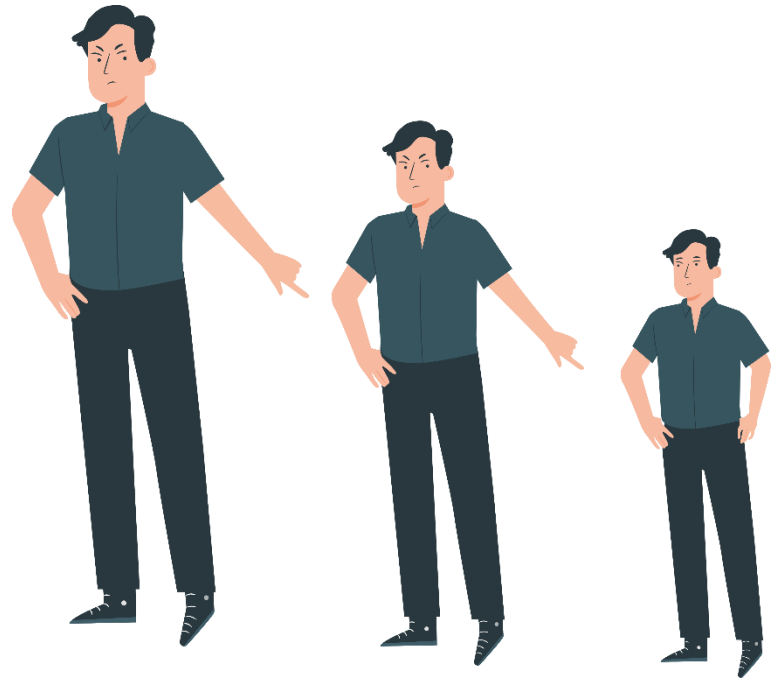
Не выстроены процессы по ИБ

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 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

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

Что и как защищать в АСУ ТП? Переосмысление концепции АСУ ТП в 2024

Алексей Петухов

Руководитель отдела развития продуктов InfoWatch ARMA

TADVISER
Государство. Бизнес. ИТ

InfoWatch ARMA — лучшее решение
по защите ИТ-систем в промышленности
по версии Tadviser (2022)

INFOWATCH® ARMA

20
лет на рынке
информационной
безопасности

30%
ежегодный рост
инвестиций
в разработку,
2020–2023

500+
сотрудников
в компании

28
патентов
на технологии

3500+
клиентов
из 12 отраслей
в 26 странах

135+
аналитических
отчётов в год

100+
технологических
партнёров

5000+
обученных
специалистов ИБ

Вызовы ИБ

Аналитика

76% интегрируют информационные технологии (ИТ) и операционные технологии (ОТ) в единую сеть

При этом

Из 400 компаний по всему миру

97% опрошенных сообщили, что атаки на ИТ инфраструктуру предприятия также затронули и ОТ.

47% атак — вымогатели

Пример.
Атака на морской порт 5 июля 2023

Грузовой порт Нагои остановил работу из-за хакерской атаки

Крупнейший в Японии грузовой порт в городе Нагоя остановил разгрузку и погрузку контейнеров в терминалах из-за кибератаки. Хакеры запустили в компьютерную систему порта вирус-вымогатель. Работы были приостановлены с утра 4 июля и, как надеются в порту, будут возобновлены к утру 6 июля. Сейчас специалисты работают над решением проблемы. Свое расследование начала полиция префектуры Айти, сообщает газета«Асахи Симбун».

Грузовой порт Нагои ежегодно обслуживает около 200 млн тонн грузов. Из-за невозможности погрузки и разгрузки в порту образовалась большая очередь из контейнеровозов. Кроме того, накопилось много контейнеров, ожидавших погрузки на суда. Как отмечает издание, если на восстановление системы уйдет больше времени, чем ожидается, серьезно пострадает перевозка грузов в первую очередь для автомобильной отрасли, а также бытовой техники и продуктов.

Источник — «Коммерсантъ», 5 июля 2023

ВИРУС-ВЫМОГАТЕЛЬ

Шифрование системы диспетчеризации

- 2 дня простоя

Пример.
Атака на движение поездов 27 августа 2023

В Польше сообщили об остановке 20 поездов из-за хакерской атаки

Wyborcza: в польском Щецине хакеры остановили поезда и включили гимн России

27 августа 2023, 04:24

120

ПОЛЬША КИБЕРАТАКИ ХАКЕРЫ ЖЕЛЕЗНЫЕ ДОРОГИ

Источник — «Известия», 27 августа 2023

ПОДМЕНА РАДИОСИГНАЛА

Аварийная остановка согласно регламенту

- 20 поездов прекратили движение

Пример.
Атака на производство 28 апреля 2023

Сообщение для наших клиентов: инцидент с кибербезопасностью

28 апреля 2023 г.

В начале января 2023 года мы подверглись серьезной кибератаке на наш бизнес. Хотя атака была обнаружена относительно быстро, и нам удалось ограничить ущерб за счет быстрого разделения сети, атака привела к шифрованию ряда наших приложений и систем хранения данных, а также повреждению сетевых устройств.

После инцидента мы постепенно восстанавливали наши сети и системы, включая восстановление некоторых приложений и файловых систем, где их невозможно было восстановить. Мы привлекли ряд специализированных

Источник — Morgan Advanced Materials, 2023

ВИРУС-ВЫМОГАТЕЛЬ

Шифрование систем хранения данных с производственными документами, планами, а также SCADA

- Оценка прямых потерь — $14 млн
- Прогноз падения годовой прибыли — 10–15%

Примеры последствий для производства по итогу анализа 2022

- Невозможность оформления производственных и транспортных документов в течение нескольких дней
- Нарушение производственных и бизнес-операций, остановка продаж
- Отключение компьютеризированного контроля производства — переход на ручной контроль и отгрузку продукции
- Остановка / простой производства
- Приостановка деятельности компании
- Большой экономический ущерб
- Нарушение доставки и логистики
- Вывод из строя ИТ-систем компании
- Сотрудники не выходили на работу несколько дней

https://www.infowatch.ru/analytics/daydzhesty-i-obzory/uscherb-i-bankrotstvo-ot-intsidentov-ib-v-proizvodstvennom-sektore

Построение системы ИБ АСУ ТП 2024

Эффективное управление организационными мерами и процессами

Автоматизация управления и реагирования

Обмен данными с ГосСОПКА, корреляция событий и формирование правил реагирования

Эшелонированная защита предприятия

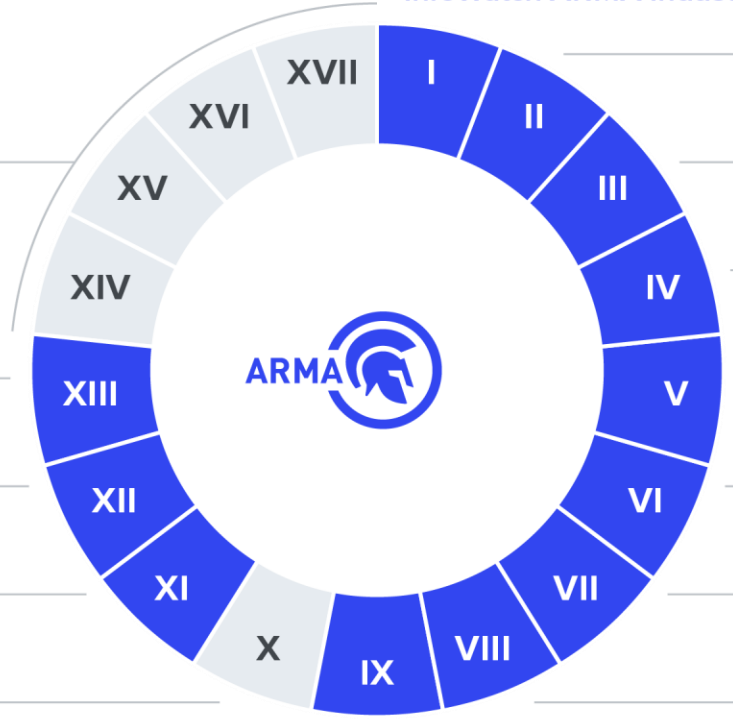
МЭ, резервное копирование, сенсор (анализ промышленных протоколов до уровня команд), защита конечных узлов (+АВ, где он применим), центр управления ИБ АСУ ТП, ...

Выполнение требований ФСТЭК и ФСБ России

Приказы ФСТЭК 17, 21, 31, 239, 235; требованиях ФСБ 368 и 282; ФЗ 187 и 152, ФЗ; указы президента РФ №250, 166 и т. д.

Люди Процессы Технологии

Основные технические решения. Приказ ФСТЭК № 239, класс 3



Организационные меры

Endpoint
InfoWatch ARMA Industrial Endpoint

Средства управления инцидентами
InfoWatch ARMA Management Console

Endpoint, МЭ
InfoWatch ARMA Industrial Firewall / Industrial Endpoint

Физическая безопасность

СОВ
InfoWatch ARMA Industrial Firewall

СОВ, МЭ
InfoWatch ARMA Industrial Firewall

Endpoint
InfoWatch ARMA Industrial Endpoint

Endpoint
InfoWatch ARMA Industrial Endpoint

СОВ, МЭ
InfoWatch ARMA Industrial Firewall

Антивирусная защита
Техническая мера ИБ

СОВ
InfoWatch ARMA Industrial Firewall

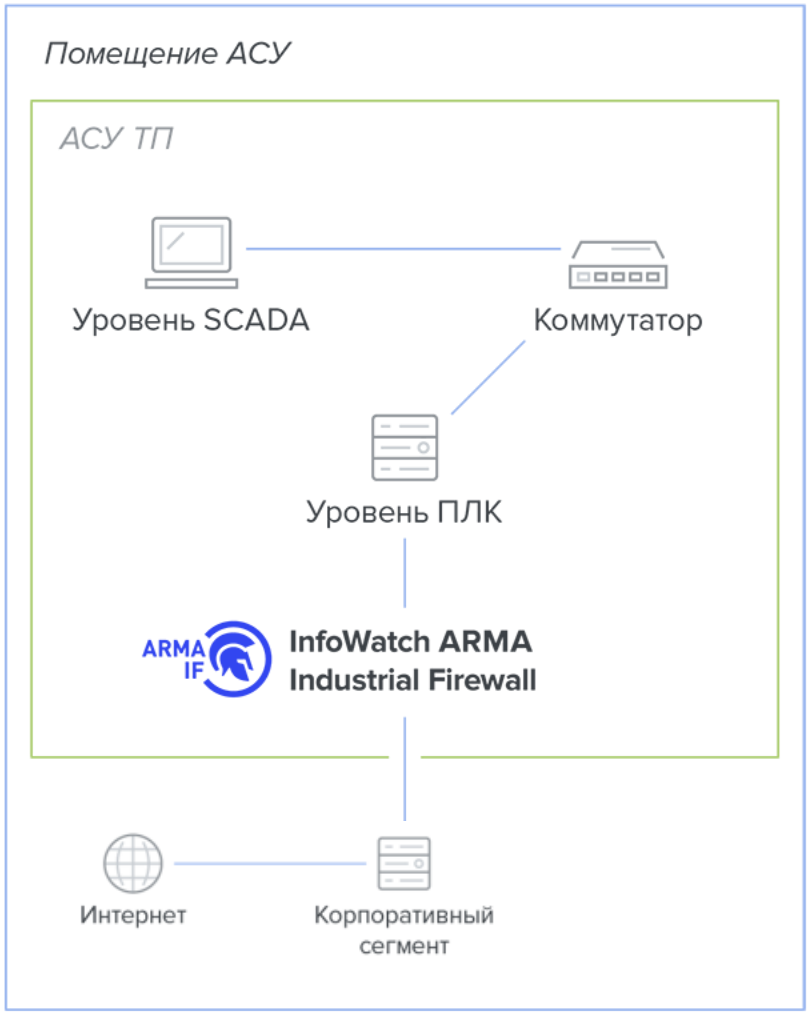
Endpoint, МЭ
InfoWatch ARMA Industrial Endpoint

МЭ
InfoWatch ARMA Industrial Firewall

Получите карту соответствия InfoWatch ARMA группам мер ФСТЭК России

Оставьте запрос на сайте
arma.infowatch.ru

Защита промышленной сети



Сценарии применения

— Удалённое защищённое соединение (ГОСТ-VPN)

— Авторизация подключаемых по сети пользователей

— Сегментирование корпоративной и/или промышленной сети

— Система обнаружения и предотвращения вторжений

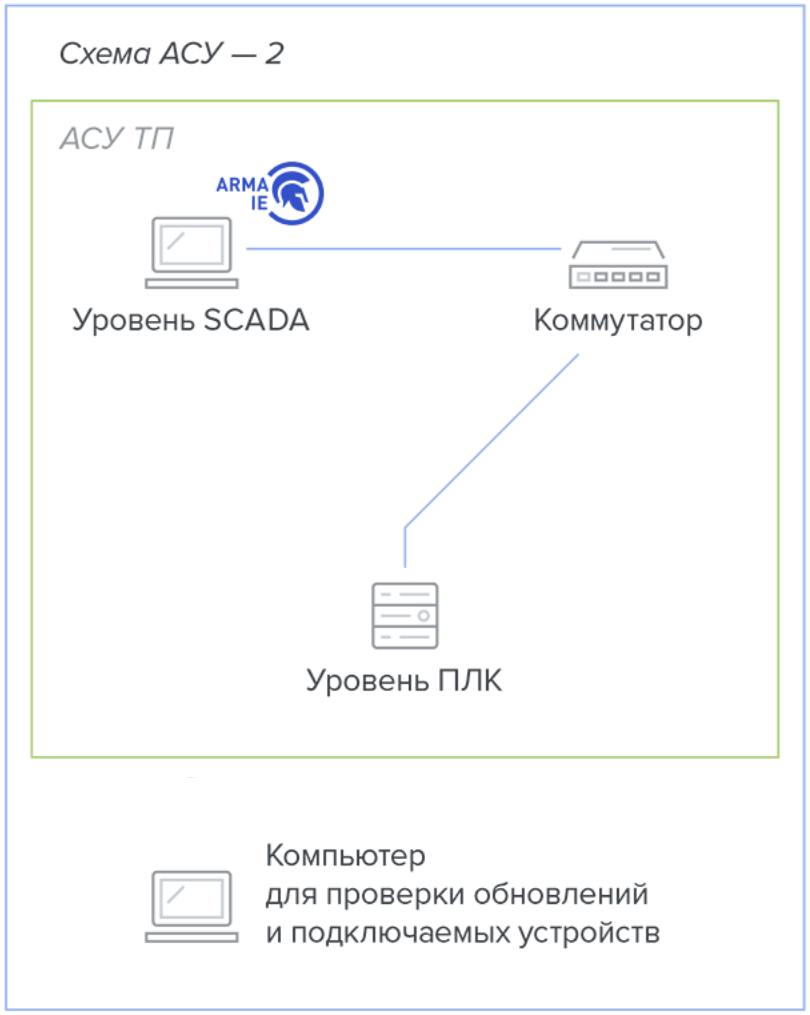
— Глубокий анализ разрешённого трафика

— Контроль доступа к web ресурсам

— DoS-защита

— Контроль/фильтрация команд для АСУ ТП

Защита рабочих станций и серверов



Сценарии применения

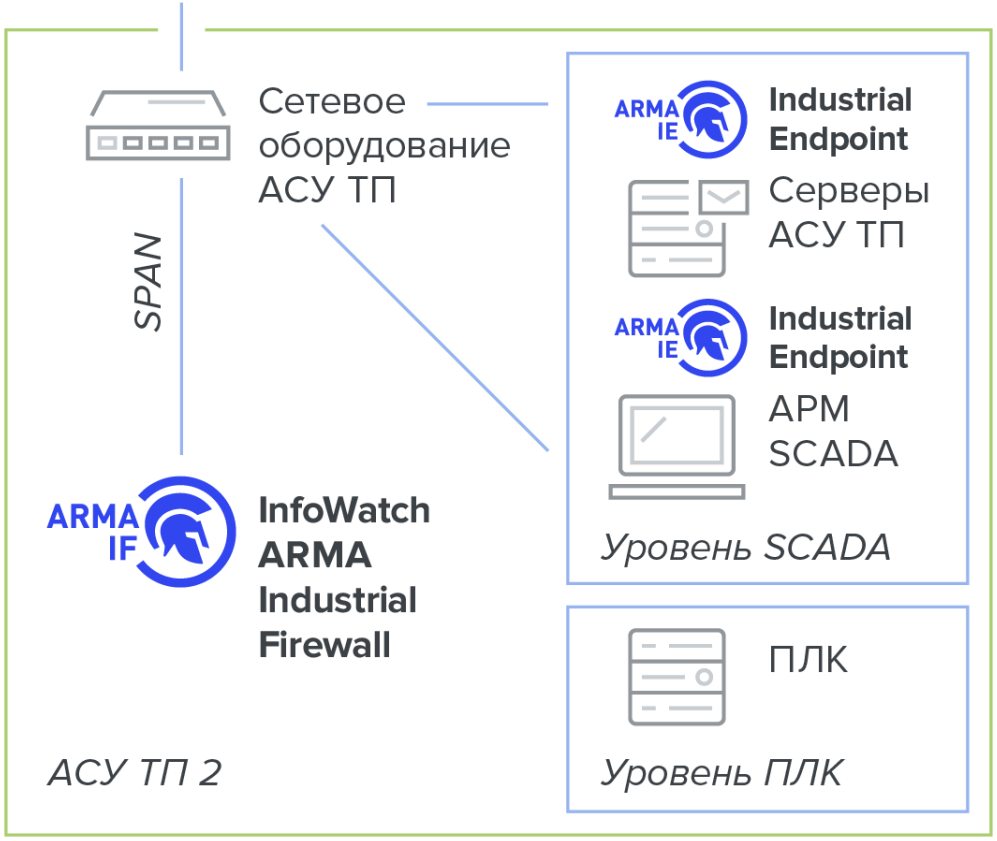
— Контроль подключаемых устройств

— Белые списки приложений

— Логирование действий и событий

\+ в рамках технологического обслуживания:
Антивирусная проверка, сканирование на уязвимости

Усиленная защита промышленной сети



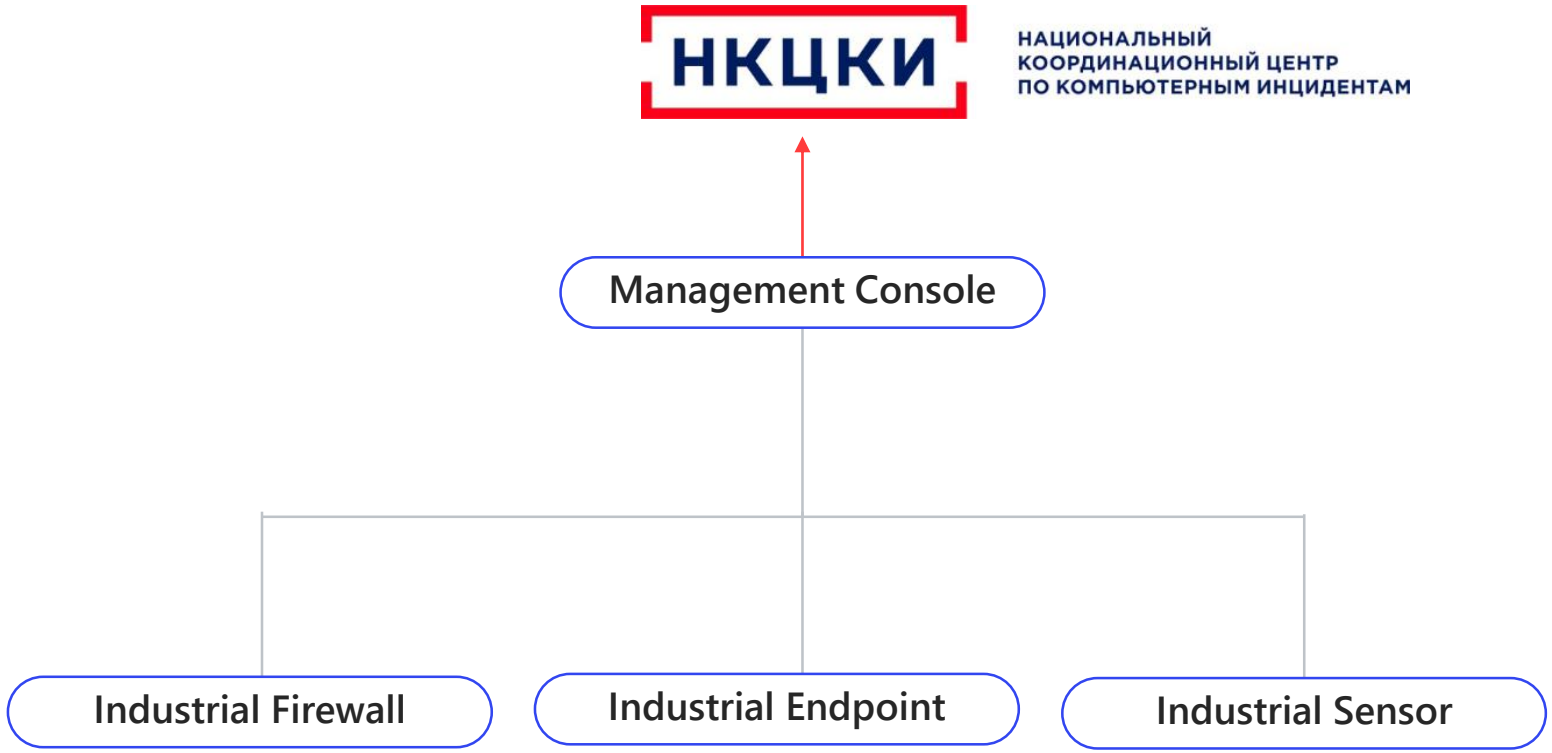
Сценарии применения

— Выявление новых устройств

— Выявление новых протоколов

— Обнаружение вторжений

Централизованное управление промышленным сегментом



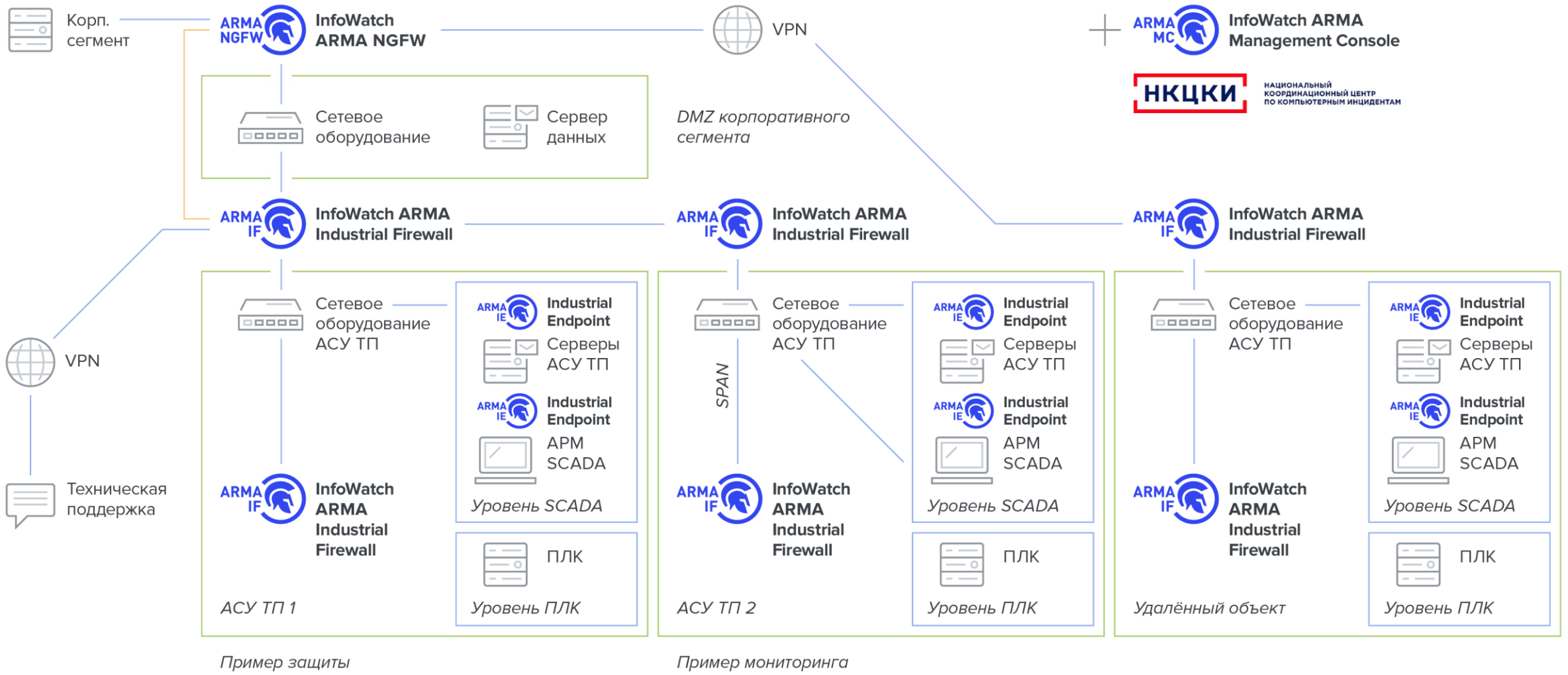
Сценарии применения

— Централизованный мониторинг

— Администрирование из 1 точки

— Взаимодействие с НКЦКИ

Единая система защиты информации на стыке IT и OT контуров



Управление системой ИБ

Пилотирование InfoWatch ARMA

Закажите пилотный проект на наших мощностях!

info@ksb-soft.ru

https://ksb-soft.ru/

+7 (8352) 322-322,
доб. 1 – коммерческий отдел

Телеграм-канал
«Мнение Интегратора»

Руководитель отдела развития продуктов InfoWatch ARMA Алексей Петухов

Телеграм-канал
Алексея Петухова

ПРИГЛАШАЕМ ПОСЕТИТЬ

КОНФЕРЕНЦИЯ

«Информационная безопасность АСУ ТП критически важных объектов»

13-14 марта, Москва Центр «Планета КВН» (ул. Шереметьевская, 2)

Доклад **13 марта**
Михаил Шипицын: **"Мониторинг в АСУ ТП: не попробуешь, не узнаешь«**

Стенд КСБ-СОФТ (**№4.3** на 3 этаже)