INFOWATCH ARMA

ОРГАНИЗАЦИОННЫЕ МЕРЫ И РОССИЙСКИЕ РЕШЕНИЯ ДЛЯ ЗАЩИТЫ АСУТП СУБЪЕКТОВ КИИ

вызовы | решения | кейсы

Алексей Петухов
Руководитель отдела по развитию бизнеса, InfoWatch ARMA

PRO автоматизацию

InfoWatch в цифрах и фактах

20
лет на рынке информационной безопасности

39
программных технологий и патентов

500+
сотрудников в компании

26
стран, вкл. СНГ, Турцию, Индию, Южную Америку и Ближний Восток

4000+
проектов из 20 отраслей в 20 странах

135+
отчётов в год выпускает ЭАЦ InfoWatch

100+
технологических партнёров

5000+
обученных специалистов ИБ

Аккредитация ЦБ РФ

Рекомендовано АРПП «Отечественный софт»

Инновация года в ИБ, 2022
CNews FORUM Кейсы

Национальная банковская премия, 2023

Лучшее ИБ-решение, 2021
TAdviser

DLP Market Guide
Первое российское DLP-решение, вошедшее в Gartner Magic Quadrant и удерживающее признание более 10 лет

Полезные данные и статистика

Экспертно-аналитический центр InfoWatch

Тенденции развития киберинцидентов АСУ ТП

Исследование кибербезопасности АСУ ТП — новые подходы

Исследование устройств АСУ ТП, уязвимых для удалённых атак

Сегодня цифровизация актуальна как никогда

76%

промышленных компаний интегрируют информационные и операционные технологии в единую сеть

Кибератаки затрагивают ИТ- и ОТ-инфраструктуру

97%

опрошенных сообщили, что атаки на ИТ инфраструктуру предприятия также затронули и ОТ. 47% атак — вымогатели

Необходимо создать и эксплуатировать систему ИБ, которая...

Построена на российских решениях

Выполняет требования регуляторов
ФСТЭК, ФСБ, Минцифры, Минпром

Эффективна

Особая роль ИБ — сделать цифровизацию проще и безопаснее. Например:

- **Обеспечить безопасный удалённый доступ**
- **Минимизировать необходимость обновлений**

  Многие обновления связаны с закрытием уязвимостей, которые ИБ-решения перекрывают
- **Повысить стабильность работы и отказоустойчивость АСУ ТП**
- **Обеспечить контроль за действиями персонала и процессами**

  Защита от ошибок и злонамеренных действий

Жизненный цикл ИБ

Модель зрелости процессов в соответствии с требованиями ISO/IEC 21827
«Инжиниринг систем безопасности — модель зрелости возможностей»

Базовые практики выполнены

- **Поручение** выполнения
- **Планирование** выполнения
- **Дисциплинарное** выполнение
- **Прослеживание** выполнения
- **Верификация** выполнения

- **Определение** стандартного процесса
- **Адаптация** стандартного процесса
- **Использование** данных
- **Выполнение** определённого процесса

- **Установление** измеримых целей качества
- **Определение** возможности процесса для достижения целей
- **Объективное** руководство выполнением

- **Установление** количественных целей эффективности процесса
- **Улучшение** эффективности процесса

Построение системы ИБ АСУ ТП — 2024

Эффективное управление организационными мерами и процессами

люди

Эшелонированная защита предприятия

системы обнаружения вторжений, песочницы, решения разных производителей для разных сегментов

Автоматизация управления и реагирования

корреляция событий и формирование правил реагирования, обмен данными с ГосСОПКА

технологии

Выполнение требований ФСТЭК и ФСБ России

приказы ФСТЭК №17, 21, 31, 239, 235; требования ФСБ №368, 282; ФЗ-187, 152; указы президента РФ №250, 166...

процессы

Информационная безопасность

INFOWATCH® ARMA

Роль ИБ в жизнедеятельности компании

Создание новой системы или процесса

Какая польза?	Какая целевая модель?	Реализация	Подготовка персонала и эксплуатация

Роль ИБ

Предоставление решений бизнес-задач при стратегическом планировании и тактическом управлении	Участие в разработке информационной, ролевой моделей взаимодействия и организационно-распорядительной документации, а также планирование ресурсов	Контроль надёжности применяемых ИТ-решений и ПАК	Защита от атак, а также человеческих, технологических и технических ошибок

Ключевые меры и процессы ИБ

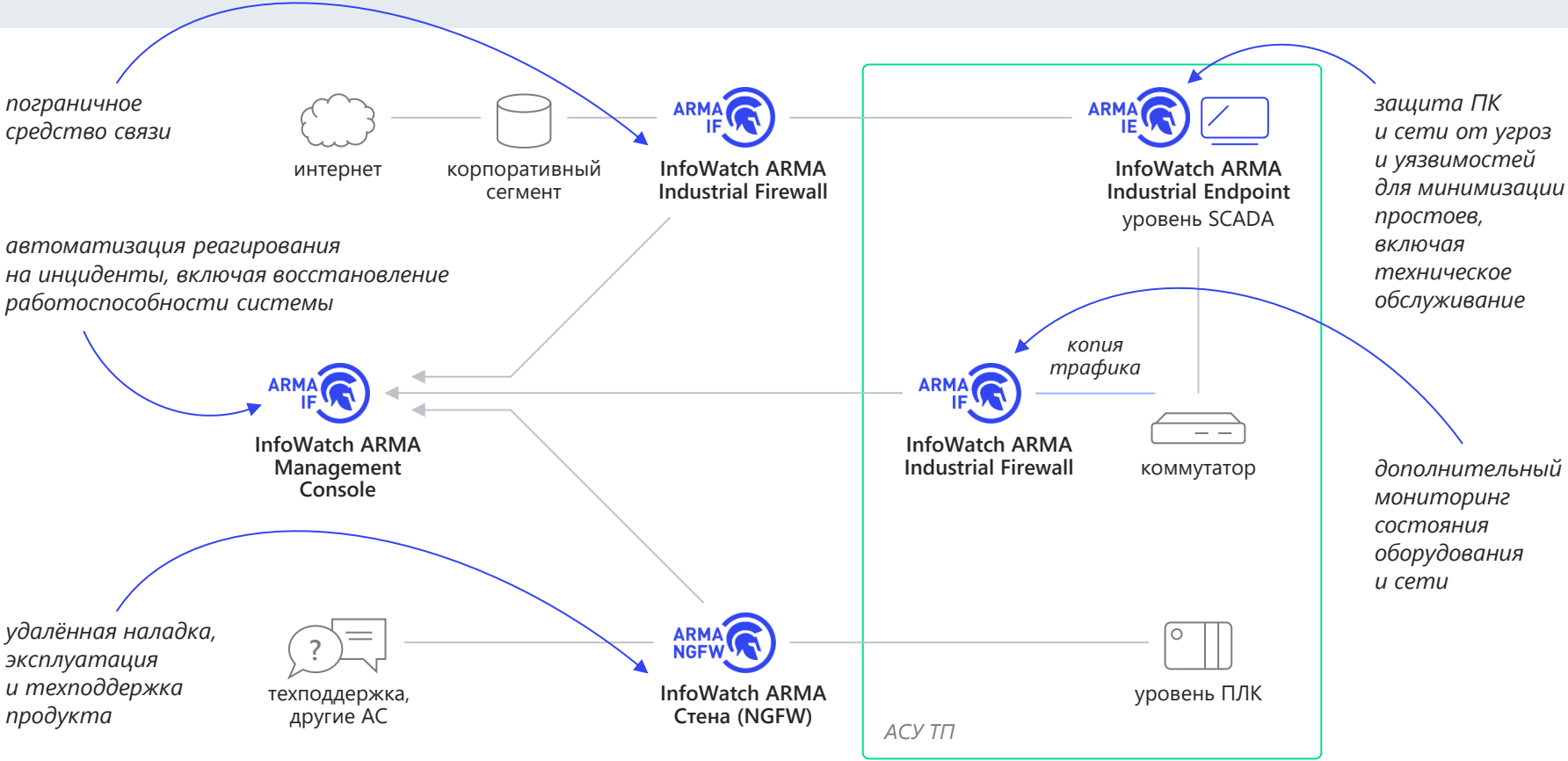
Идентификация и аутентификация
Управление доступом
Контроль подключаемых устройств
Аудит ИБ
Защита устройств
Защита сети
Защита программных приложений
Защита баз данных
Централизованный мониторинг событий
Управление обновлениями ПО
Резервное копирование
Регламент действий при внештатных ситуациях
Обучение пользователей и администраторов
*Взаимодействие с регулятором
**Безопасная разработка ПО

- описание процесса
- наличие ответственных
- осведомлённость сотрудников
- документирование
- интерактивность

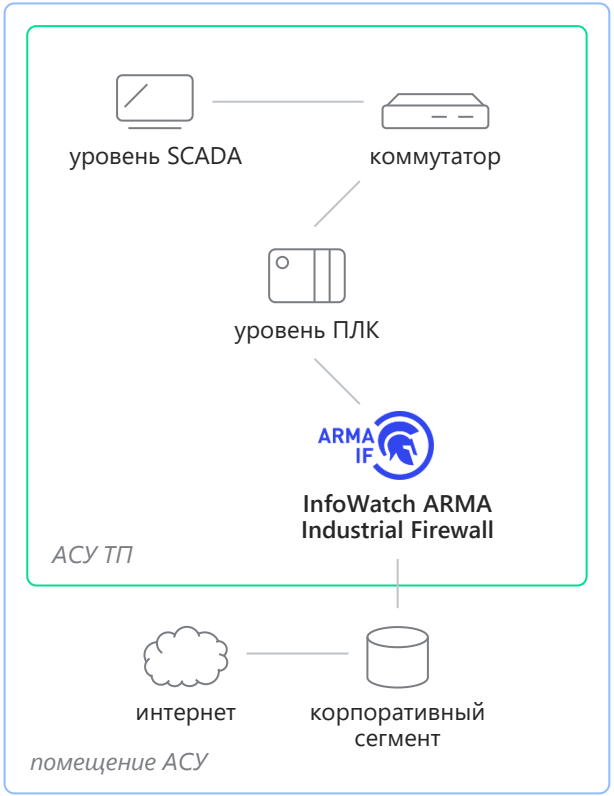
Целевая схема ИБ на примере модели зрелости IIoT

Достижение зрелости безопасности	**Управление**	**Стратегия и руководство**	Руководство программой безопасности
			Обеспечение соответствия внешним требованиям
		Угрозы и риски	Моделирование угроз
			Подход к управлению рисками
		Поставки и внешние зависимости	Управление безопасностью поставок ИТ-компонентов
			Управление зависимостями от внешних ИТ-сервисов
	Внедрение	**Управление доступом**	Управление учётными записями
			Контроль доступа
		Защита активов	Управление активами, изменениями и конфигурацией
			Физическая защита активов
		Защита данных	Модель и политика защиты данных
			Реализация механизмов защиты данных
	Укрепление	**Уязвимости и обновления безопасности**	Поиск и оценка уязвимостей
			Управление обновлениями безопасности
		Ситуационная осведомлённость	Мониторинг и отслеживание событий ИБ
			Поддержание осведомлённости о состоянии ИБ
		Реагирование и восстановление	План реагирования на инциденты безопасности
			Поддержание непрерывной работы и восстановление

Сценарии применения решений ИБ для решения базовых задач



Защита промышленной сети



Сценарии применения

— Удалённое защищённое соединение (ГОСТ-VPN)

— Контроль подключений по протоколам удалённого доступа

— Сегментирование корпоративной и / или промышленной сети

— Авторизация подключаемых по сети пользователей

— Система обнаружения и предотвращения вторжений

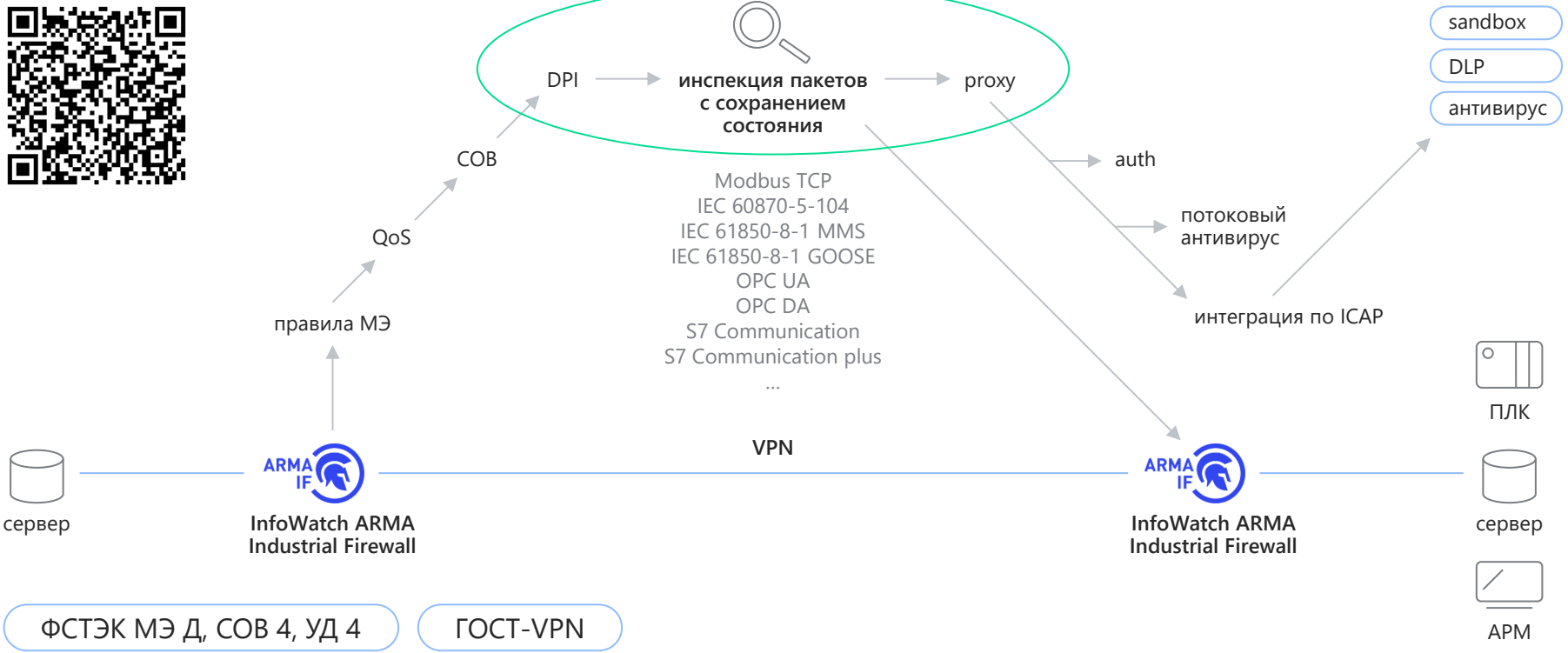
— DoS-проверка

— Запрет всех подключений, кроме разрешённых связей с другими системами автоматизации и управления производством

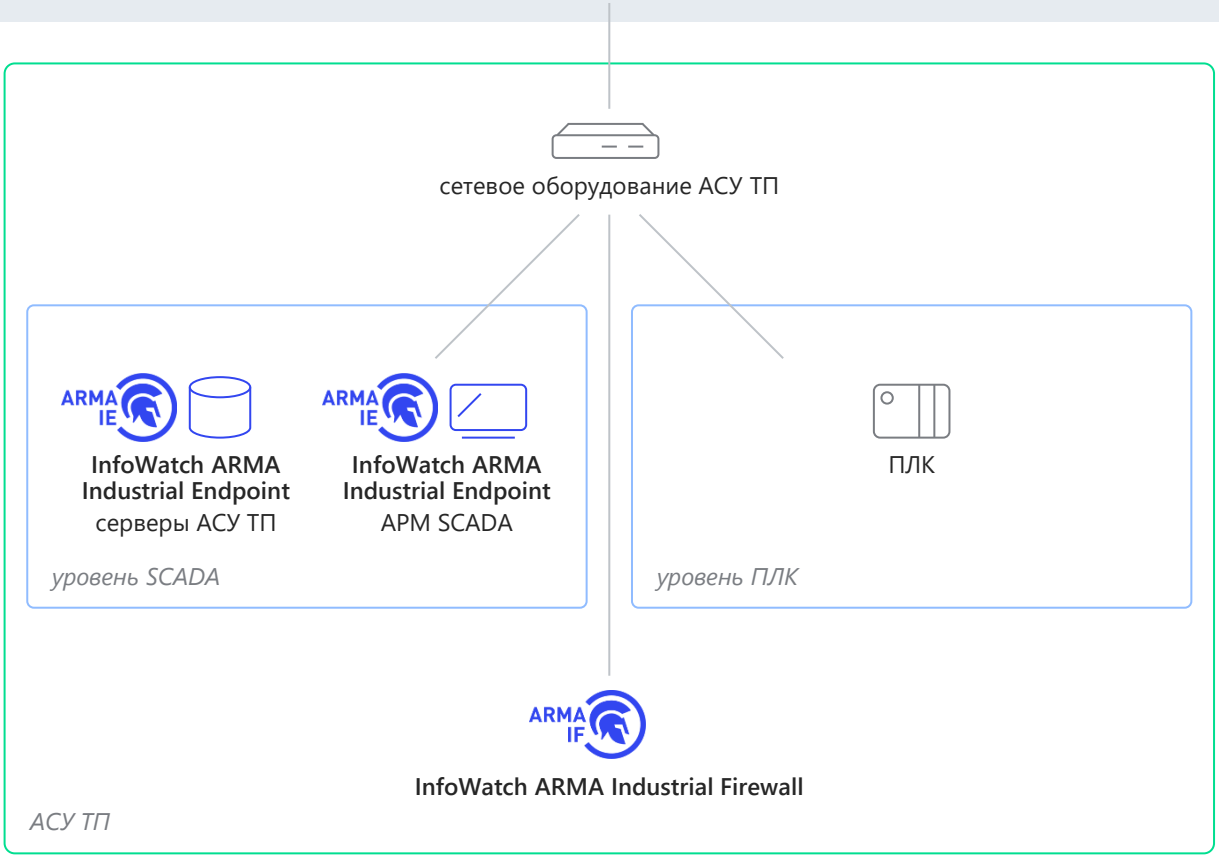
— Пограничный маршрутизатор для АСУ ТП

— Контроль / фильтрация команд для АСУ ТП

Глубокая экспертиза инспектирования промышленных данных



Усиленная защита промышленной сети



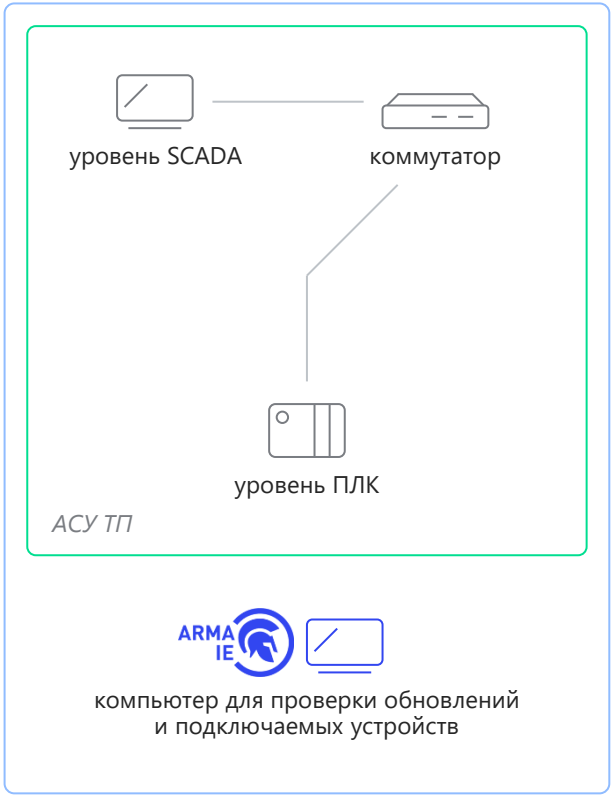
Сценарии применения

— Выявление новых устройств

— Выявление новых протоколов

— Обнаружение вторжений

Защита рабочих станций и серверов



Сценарии применения

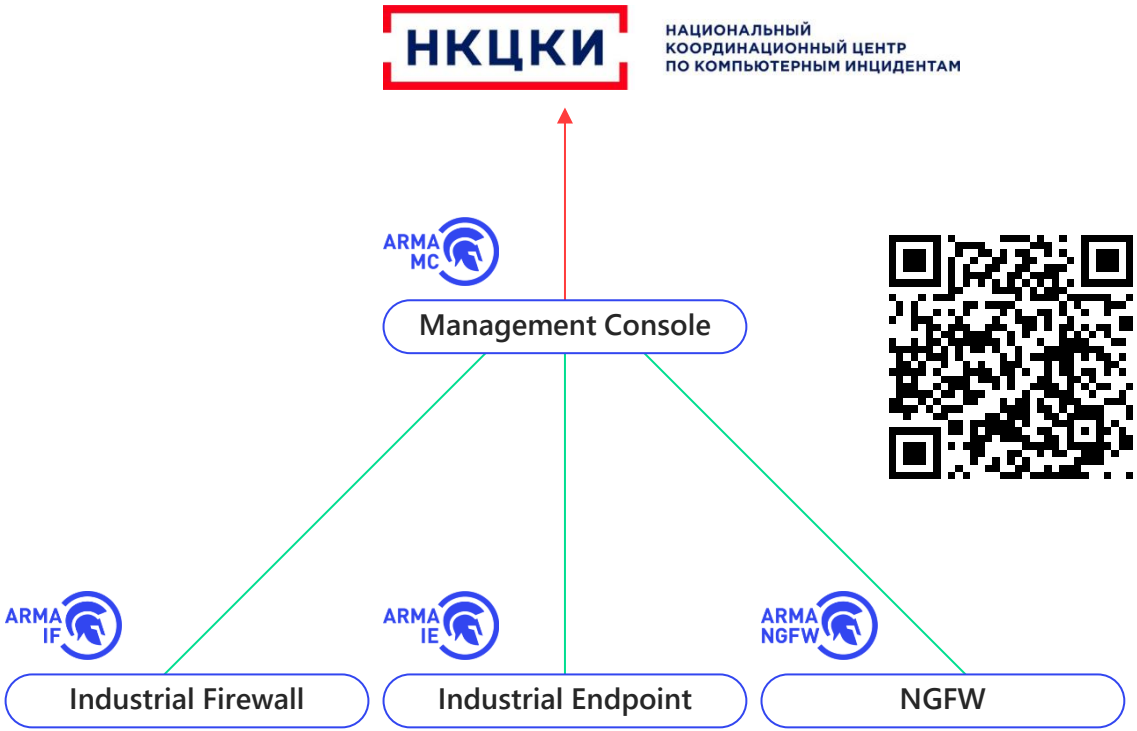
— Контроль подключаемых устройств

— Белые списки приложений

— Логирование действий и событий

антивирусная проверка и сканирование на уязвимости
в рамках технологического обслуживания

Централизованное управление



Сценарии применения

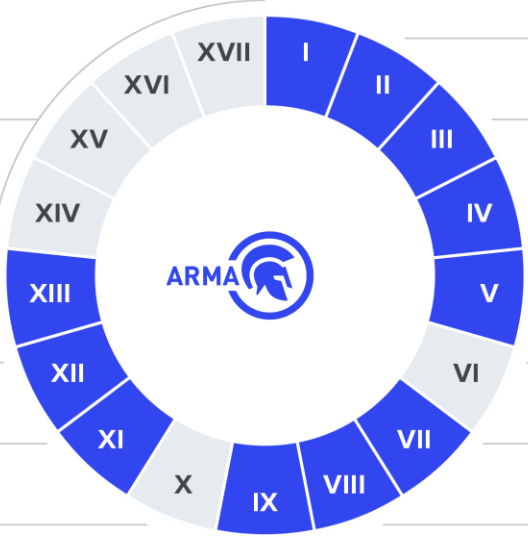
— Централизованный мониторинг

— Администрирование из одной точки

— Взаимодействие с НКЦКИ

Интегрируемость для комплексного решения

закрытие до 90% технических мер приказа ФСТЭК России №239



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

МЭ
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

СОВ
InfoWatch ARMA Industrial Firewall

Endpoint, МЭ
InfoWatch ARMA Industrial Endpoint

Пример реализации

INFOWATCH® ARMA

РАДЫ ПОМОЧЬ

arma.infowatch.ru

/InfoWatchOut /InfoWatch

PRO автоматизацию