INFOWATCH®

ARMA

КАРТА РЕАЛИЗАЦИИ ТЕХНИЧЕСКИХ МЕР ПРИКАЗА № 239 ФСТЭК РОССИИ

На примере продуктов InfoWatch ARMA

Данный документ не заменяет и не уточняет требования нормативных и методических документов по защите информации. Цель документа — обзор решения для реализации мер безопасности. В качестве примера мы рассматриваем комплексную систему для обеспечения кибербезопасности АСУ ТП — InfoWatch ARMA, которая относится к реализации приведённых мер безопасности. Выбор организационных и технических мер для обеспечения безопасности конкретного объекта КИИ определяется в ходе подготовки технорабочего проекта.

Термины и сокращения

SACM	Service Asset and Configuration Management: процесс, ответственный за управление конфигурациями и управление активами
ППО	Прикладное ПО
СОЕВ	Система обеспечения единого времени
ОС	Операционная система (сертифицированная)
СЗИ от НСД	Средства защиты информации от несанкционированного доступа
IDM	Система управления доступом
МЭ	Межсетевой экран
DLP	Система защиты информации от утечки
СКЗИ	Система криптографической защиты информации
МДЗ	Модуль доверенной загрузки
СКУД	Система контроля и управления доступом
СОВ	Система обнаружения вторжений
СПВ	Система предотвращения вторжений
СОА	Система обнаружения атак
SIEM	Security information and event management: система управления информационной безопасностью и событиями безопасности
Backup / recovery	Резервное копирование и восстановление данных
КИТСО	Комплекс инженерно-технических средств охраны
Honeypot	Ресурс-приманка для злоумышленников
MDM	Mobile device management: управление мобильными устройствами
VPN	Виртуальная частная сеть
ЭЦП	Электронно-цифровая подпись

Обозначение и номер меры	Описание меры	Категории КИИ, для которой мера обязательна			Чем возможно обеспечение меры		Решения InfoWatch
					Организационная мера	Класс технического решения	
I. Идентификация и аутентификация (ИАФ)							
ИАФ.0	Разработка политики идентификации и аутентификации	1	2	3	Организационная мера	—	—
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга	InfoWatch ARMA Industrial Firewall
ИАФ.2	Идентификация и аутентификация устройств	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	InfoWatch ARMA Industrial Firewall
ИАФ.3	Управление идентификаторами	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	InfoWatch ARMA Industrial Firewall
ИАФ.4	Управление средствами аутентификации	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга	InfoWatch ARMA Industrial Firewall
ИАФ.5	Идентификация и аутентификация внешних пользователей	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	InfoWatch ARMA Industrial Firewall
ИАФ.6	Двусторонняя аутентификация				—	ОС, IdM / СЗИ от НСД / система мониторинга	—
ИАФ.7	Защита аутентификационной информации при передаче	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга	InfoWatch ARMA Industrial Firewall
II. Управление доступом (УПД)							

УПД.0	Разработка политики управления доступом	1	2	3	Организационная мера	—	—
УПД.1	Управление учётными записями пользователей	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга	**InfoWatch ARMA Industrial Firewall**
УПД.2	Реализация политик управления доступа	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	**InfoWatch ARMA Industrial Firewall**
УПД.3	Доверенная загрузка	1	2		—	Средства доверенной загрузки	—
УПД.4	Разделение полномочий (ролей) пользователей	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	**InfoWatch ARMA Industrial Firewall**
УПД.5	Назначение минимально необходимых прав и привилегий	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	**InfoWatch ARMA Industrial Firewall**
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга	**InfoWatch ARMA Industrial Firewall**
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам				—	ОС, IdM / СЗИ от НСД / система мониторинга	—
УПД.8	Оповещение пользователя при успешном входе предыдущем доступе к информацион-ной (автоматизированной) системе				—	ОС, IdM / СЗИ от НСД / система мониторинга	—
УПД.9	Ограничение числа параллельных сеансов доступа	1			—	ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	**InfoWatch ARMA Industrial Firewall**
УПД.10	Блокирование сеанса доступа пользователя при неактивности	1	2	3	—	Штатные средства АСУ / ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	**InfoWatch ARMA Industrial Firewall**
УПД.11	Управление действиями пользователей до идентификации и аутентификации	1	2	3	—	ОС, IdM / СЗИ от НСД / система мониторинга / МЭ	**InfoWatch ARMA Industrial Firewall**

УПД.12	Управление атрибутами безопасности				—	ОС, IdM / СЗИ от НСД	—
УПД.13	Реализация защищенного удалённого доступа	1	2	3	—	МЭ / СКЗИ	**InfoWatch ARMA Industrial Firewall**
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
III. Ограничение программной среды (ОПС)							
ОПС.0	Разработка политики ограничения программной среды	1	2		Организационная мера	—	—
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	1			—	Управление запуском (обращениями) компонентов программного обеспечения	**InfoWatch ARMA Industrial Endpoint**
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения	1	2		—	Управление запуском (обращениями) компонентов программного обеспечения	**InfoWatch ARMA Industrial Endpoint**
ОПС.3	Управление временными файлами				—	СЗИ НСД	—
IV. Защита машинных носителей информации (ЗНИ)							
ЗНИ.0	Разработка политики защиты машинных носителей информации	1	2	3	Организационная мера	—	—
ЗНИ.1	Учёт машинных носителей информации	1	2	3	—	СЗИ НСД	—
ЗНИ.2	Управление физическим доступом к машинным носителям информации	1	2	3	—	СЗИ НСД	—

ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				Организационная мера	СЗИ НСД / СКЗИ	—
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации				—	СЗИ НСД / СКЗИ	—
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	1	2	3	—	СЗИ НСД / СКЗИ	**InfoWatch ARMA Industrial Endpoint**
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	1			—	СЗИ НСД / СКЗИ	**InfoWatch ARMA Industrial Endpoint**
ЗНИ.7	Контроль подключения машинных носителей информации	1	2	3	—	СЗИ НСД / СКЗИ	**InfoWatch ARMA Industrial Endpoint**
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	1	2	3	Организационная мера	—	—
V. Аудит безопасности (АУД)							
АУД.0	Разработка политики аудита безопасности	1	2	3	Организационная мера	—	—
АУД.1	Инвентаризация информационных ресурсов	1	2	3	—	СЗИ НСД / МЭ / сканер защищённости	**InfoWatch ARMA Industrial Firewall**
АУД.2	Анализ уязвимостей и их устранение	1	2	3	—	СЗИ НСД / МЭ / сканер защищённости	—
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	1	2	3	—	Система единого времени	—
АУД.4	Регистрация событий безопасности	1	2	3	—	МЭ / СОВ / антивирус / СЗИ НСД	**InfoWatch ARMA Industrial Firewall**

АУД.5	Контроль и анализ сетевого трафика	1			—	МЭ / СОВ	**InfoWatch ARMA Industrial Firewall**
АУД.6	Защита информации о событиях безопасности	1	2	3	Организационная мера	Реализуется внутри СЗИ	**InfoWatch ARMA Industrial Firewall**
АУД.7	Мониторинг безопасности	1	2	3	Организационная мера	Реализуется внутри СЗИ	**InfoWatch ARMA Industrial Firewall**
АУД.6	Защита информации о событиях безопасности	1	2	3	—	Реализуется внутри СЗИ	—
АУД.7	Мониторинг безопасности	1	2	3	—	Реализуется внутри СЗИ	—
АУД.8	Реагирование на сбои при регистрации событий безопасности	1	2	3	Организационная мера	—	—
АУД.9	Анализ действий пользователей	1			—	МЭ / СОВ / антивирус / СЗИ НСД	**InfoWatch ARMA Industrial Firewall**
АУД.10	Проведение внутренних аудитов	1	2	3	Организационная мера	—	—
АУД.11	Проведение внешних аудитов				Организационная мера	—	—
VI. Антивирусная защита (АВЗ)							
АВЗ.0	Регламентация правил и процедур антивирусной защиты	1	2	3	Организационная мера	—	—
АВЗ.1	Реализация антивирусной защиты	1	2	3	—	Антивирус	—

АВЗ.2	Антивирусная защита электронной почты и иных сервисов	1	2	3	—	Антивирус	—
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	1			—	Антивирус	—
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	1	2	3	—	Антивирус	—
АВЗ.5	Использование средств антивирусной защиты различных производителей	1			—	Антивирус	—
VII. Предотвращение вторжений (компьютерных атак) (СОВ)							
СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)	1	2		Организационная мера	—	—
СОВ.1	Обнаружение и предотвращение компьютерных атак	1	2		—	СОВ	**InfoWatch ARMA Industrial Firewall**
СОВ.2	Обновление базы решающих правил	1	2		—	СОВ	**InfoWatch ARMA Industrial Firewall**
VIII. Обеспечение целостности (ОЦЛ)							
ОЦЛ.0	Разработка политики обеспечения целостности	1	2	3	Организационная мера	—	—
ОЦЛ.1	Контроль целостности программного обеспечения	1	2	3	—	Антивирус / СЗИ НСД	**InfoWatch ARMA Industrial Endpoint**
ОЦЛ.2	Контроль целостности информации				—	Антивирус / СЗИ НСД	**InfoWatch ARMA Industrial Endpoint**

ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	1			—	Антивирус / СЗИ НСД	**InfoWatch ARMA Industrial Firewall**
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	1	2		—	Антивирус / СЗИ НСД	**InfoWatch ARMA Industrial Firewall**
ОЦЛ.5	Контроль ошибочных действий по вводу и (или) передаче информации и предупреждение пользователей об этих действиях	1	2		—	Антивирус / СЗИ НСД	**InfoWatch ARMA Industrial Firewall**
ОЦЛ.6	Обезличивание и (или) деидентификация информации				—	Антивирус / СЗИ НСД	—
IX. Обеспечение доступности (ОДТ)							
ОДТ.0	Разработка политики обеспечения доступности	1	2	3	Организационная мера	—	—
ОДТ.1	Использование отказоустойчивых технических средств	1	2		—	—	**InfoWatch ARMA Industrial Firewall**
ОДТ.2	Резервирование средств и систем	1	2		—	—	**InfoWatch ARMA Industrial Firewall**
ОДТ.3	Контроль безотказного функционирования средств и систем	1	2		—	—	**InfoWatch ARMA Industrial Firewall**
ОДТ.4	Резервное копирование информации	1	2	3	—	Системы резервирования	**InfoWatch ARMA Industrial Firewall**
ОДТ.5	Обеспечение возможности восстановления информации	1	2	3	—	Системы резервирования	**InfoWatch ARMA Industrial Firewall**
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	1	2	3	—	Системы резервирования	**InfoWatch ARMA Industrial Firewall**

ОДТ.7	Кластеризация информационной (автоматизированной) системы				—	—	InfoWatch ARMA Industrial Firewall
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	1	2	3	Организационная мера	—	—
X. Защита технических средств и систем (ЗТС)							
ЗТС.0	Разработка политики защиты технических средств и систем	1	2	3	Организационная мера	—	—
ЗТС.2	Организация контролируемой зоны	1	2	3	Организационная мера	—	—
ЗТС.3	Управление физическим доступом	1	2	3	Организационная мера	—	—
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр	1	2	3	Организационная мера	—	—
ЗТС.5	Защита от внешних воздействий	1	2	3	Организационная мера	—	—
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации				Организационная мера	—	—
XI. Защита информационной (автоматизированной) системы и её компонентов (ЗИС)							
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и её компонентов	1	2	3	Организационная мера	—	—
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	1	2	3	Организационная мера	—	—

ЗИС.2	Защита периметра информационной (автоматизированной) системы	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.4	Сегментирование информационной (автоматизированной) системы	1	2		—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.5	Организация демилитаризованной зоны	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.6	Управление сетевыми потоками	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения («песочница»)				—	«Песочница»	—
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.9	Создание гетерогенной среды				—	—	—
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем				—	—	—
ЗИС.11	Предотвращение задержки или прерывания процессов с высоким приоритетом со стороны процессов с низким приоритетом				—	—	—
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти				—	—	—
ЗИС.13	Защита неизменяемых данных	1	2		—	СЗИ НСД	**InfoWatch ARMA Industrial Endpoint**

ЗИС.14	Использование неперезаписываемых машинных носителей информации				—	—	—
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек				—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.16	Защита от спама	1	2		—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.17	Защита информации от утечек				—	DLP	—
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещённых к использованию				—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.19	Защита информации при её передаче по каналам связи	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.20	Обеспечение доверенных канала и маршрута	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.21	Запрет несанкционированной удалённой активации периферийных устройств	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами				—	МЭ / СЗИ НСД / штатные средства АСУ	—
ЗИС.23	Контроль использования мобильного кода				—	Специальные средства	—
ЗИС.24	Контроль передачи речевой информации				—	МЭ	—
ЗИС.25	Контроль передачи видеоинформации				—	МЭ	—

ЗИС.26	Подтверждение происхождения источника информации				—	МЭ / СКЗИ	—
ЗИС.27	Обеспечение подлинности сетевых соединений	1	2		—	МЭ / СКЗИ	**InfoWatch ARMA Industrial Firewall**
ЗИС.28	Исключение возможности отрицания отправки информации				—	МЭ / СКЗИ	—
ЗИС.29	Исключение возможности отрицания получения информации				—	МЭ / СКЗИ	—
ЗИС.30	Использование устройств терминального доступа				Организационная мера	—	—
ЗИС.31	Защита от скрытых каналов передачи информации				Организационная мера	—	—
ЗИС.32	Защита беспроводных соединений	1	2	3	—	Специальные средства	—
ЗИС.33	Исключение доступа через общие ресурсы	1			—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.34	Защита от угроз отказа в обслуживании (DOS- / DDOS-атак)	1	2	3	—	МЭ / специальные средства	**InfoWatch ARMA Industrial Firewall**
ЗИС.35	Управление сетевыми соединениями	1	2	3	—	МЭ	**InfoWatch ARMA Industrial Firewall**
ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем				—	Honeypot	—
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)				Организационная мера +	Штатные средства АСУ	—

ЗИС.38	Защита информации при использовании мобильных устройств	1	2	3	—	Специальные средства	—
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	1	2	3	—	Штатные средства АСУ	—
XII. Реагирование на компьютерные инциденты (ИНЦ)							
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	1	2	3	Организационная мера	—	—
ИНЦ.1	Выявление компьютерных инцидентов	1	2	3	—	Средства управления инцидентами / SIEM	**InfoWatch ARMA Management Console**
ИНЦ.2	Информирование о компьютерных инцидентах	1	2	3	—	Средства управления инцидентами / SIEM	**InfoWatch ARMA Management Console**
ИНЦ.3	Анализ компьютерных инцидентов	1	2	3	—	Средства управления инцидентами / SIEM	**InfoWatch ARMA Management Console**
ИНЦ.4	Устранение последствий компьютерных инцидентов	1	2	3	Организационная мера +	—	—
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	1	2	3	Организационная мера	—	—
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	1	2	3	—	Средства управления инцидентами / SIEM	**InfoWatch ARMA Management Console**
XIII. Управление конфигурацией (УКФ)							
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы	1	2	3	Организационная мера	—	—

УКФ.2	Управление изменениями	1	2	3	—	—	—
УКФ.3	Установка (инсталляция) только разрешённого к использованию программного обеспечения	1	2	3	—	Endpoint	**InfoWatch ARMA Industrial Endpoint**
УКФ.4	Контроль действий по внесению изменений				—	Endpoint	—

XIV. Управление обновлениями программного обеспечения (ОПО)

ОПО.0	Разработка политики управления обновлениями программного обеспечения	1	2	3	Организационная мера	—	—
ОПО.1	Поиск и получение обновлений программного обеспечения от доверенного источника	1	2	3	Организационная мера	—	—
ОПО.2	Контроль целостности обновлений программного обеспечения	1	2	3	Организационная мера	—	—
ОПО.3	Тестирование обновлений программного обеспечения	1	2	3	Организационная мера	—	—
ОПО.4	Установка обновлений программного обеспечения	1	2	3	Организационная мера	—	—

XV. Планирование мероприятий по обеспечению безопасности (ПЛН)

ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации	1	2	3	Организационная мера	—	—
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	1	2	3	Организационная мера	—	—

ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	1	2	3	Организационная мера	—	—

XVI. Обеспечение действий в нештатных ситуациях (ДНС)

ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	1	2	3	Организационная мера	—	—
ДНС.1	Разработка плана действий в нештатных ситуациях	1	2	3	Организационная мера	—	—
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	1	2	3	Организационная мера	—	—
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций	1	2		Организационная мера	—	—
ДНС.4	Резервирование программного обеспечения, тех. средств, каналов связи на случай возникновения нештатных ситуаций	1	2		Организационная мера	—	—
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возн. нештатных ситуаций	1	2	3	Организационная мера	—	—
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения				Организационная мера	—	—

XVII. Информирование и обучение персонала (ИПО)

ИПО.0	Разработка политики информирования и обучения персонала	1	2	3	Организационная мера	—	—
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	1	2	3	Организационная мера	—	—

ИПО.2	Обучение персонала правилам безопасной работы	1	2	3	Организационная мера	—	—
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы	1	2		Организационная мера	—	—
ИПО.4	Контроль осведомлённости персонала об угрозах безопасности информации и о правилах безопасной работы	1	2	3	Организационная мера	—	—

«+» — мера обеспечения безопасности включена в базовый набор мер для соответствующей категории значимого объекта.

Меры обеспечения безопасности, не обозначенные знаком «+», применяются при адаптации и дополнении базового набора мер, а также при разработке компенсирующих мер в значимом объекте критической информационной инфраструктуры соответствующей категории значимости.