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 продукт InfoWatch ARMA Industrial Firewall, который 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

InfoWatch ARMA в «системе координат» ваших объектов КИИ

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Чем возможно обеспечение меры		Решения InfoWatch	Комментарий
		3	2	1	Организационная мера	Класс технических решений		
I. Идентификация и аутентификация (ИАФ)								
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+	+	+	Организационная мера	—	—	—
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+	—	ОС, IDM	—	—
						СЗИ от НСД	—	Разграничение прав доступа пользователей к файлам
						Система мониторинга	—	Контроль инициируемых пользователями процессов
ИАФ.2	Идентификация и аутентификация устройств	+	+	+	—	ОС, IDM	—	—
						СЗИ от НСД	—	Ограничение возможности использования устройств
						МЭ	**InfoWatch ARMA Industrial Firewall**	Использование портала авторизации, идентификации устройств по IP- и MAC-адресам
ИАФ.3	Управление идентификаторами	+	+	+	—	ОС, IDM СЗИ от НСД	—	—
						МЭ	**InfoWatch ARMA Industrial Firewall**	В случае использования портала авторизации для внешних по отношению к АСУ пользователей возможно управление идентификаторами

ИАФ.4	Управление средствами аутентификации	+	+	+	—	ОС, IDM СЗИ от НСД	—	—
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+	—	ОС, IDM СЗИ от НСД	—	—
						МЭ	**InfoWatch ARMA Industrial Firewall**	—
						DLP	—	Поддержка протоколов LDAP / OpenLDAP
ИАФ.6	Двусторонняя аутентификация				—	ОС, IDM СЗИ от НСД	—	—
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+	—	ОС	—	—
						СЗИ от НСД, в т. ч. СКЗИ	—	Шифрование
						МЭ	**InfoWatch ARMA Industrial Firewall**	—

II. Управление доступом (УПД)

УПД.0	Регламентация правил и процедур управления доступом	+	+	+	Организацион-ная мера	—	—	—
УПД.1	Управление учётными записями пользователей	+	+	+	Организацион-ная мера+	ОС СЗИ от НСД	—	—
УПД.2	Реализация модели управления доступом	+	+	+	—	СЗИ от НСД	—	—

УПД.2	Реализация модели управления доступом	+	+	+	—	МЭ	**InfoWatch ARMA Industrial Firewall**	Портал авторизации позволяет настраивать параметры доступа пользователей к ресурсам
УПД.3	Доверенная загрузка		+	+	—	СЗИ от НСД, в т. ч. МДЗ	—	—
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+	Организацион-ная мера+	ОС	—	—
						СЗИ от НСД	—	Разграничение прав доступа пользователей к файлам
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+	Организацион-ная мера+	ОС	—	—
						СЗИ от НСД	—	Разграничение уровня доступа
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+	—	ОС СЗИ от НСД	—	—
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам				—	ОС СЗИ от НСД	—	—
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе				—	ОС СЗИ от НСД	—	—
УПД.9	Ограничение числа параллельных сеансов доступа			+	—	ОС СЗИ от НСД	—	—
						МЭ	**InfoWatch ARMA Industrial Firewall**	Портал авторизации позволяет установить ограничение на параллельные сеансы доступа

УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	+	+	—	ОС СЗИ от НСД	—	—
						МЭ	**InfoWatch ARMA Industrial Firewall**	—
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	+	+	—	МЭ	**InfoWatch ARMA Industrial Firewall**	—
УПД.12	Управление атрибутами безопасности				—	СЗИ от НСД	—	—
						СКЗИ	—	Шифрование
УПД.13	Реализация защищённого удаленного доступа	+	+	+	—	СКЗИ (VPN)	—	—
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+	—	СКЗИ (VPN)	—	—
						МЭ	**InfoWatch ARMA Industrial Firewall**	—
III. Ограничение программной среды (ОПС)									
ОПС.0	Регламентация правил и процедур ограничения программной среды		+	+	Организацион-ная мера	—	—	—
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			+	—	СЗИ от НСД	**InfoWatch ARMA Endpoint**	Контроль целостности и запуска ПО
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		+	+	—	СЗИ от НСД	**InfoWatch ARMA Endpoint**	Контроль целостности и запуска ПО

ОПС.3	Управление временными файлами				—	СЗИ от НСД	—	—
IV. Защита машинных носителей информации (ЗНИ)								
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации	+	+	+	Организационная мера	—	—	—
ЗНИ.1	Учёт машинных носителей информации	+	+	+	Организационная мера+	СЗИ от НСД	**InfoWatch ARMA Endpoint**	СЗИ от НСД — в части учёта машинных носителей, используемых в защищаемой АС
ЗНИ.2	Управление физическим доступом к машинным носителям информации	+	+	+	Организационная мера+	СКУД	—	—
						СЗИ от НСД	—	Контроль использования внешних устройств и съёмных носителей
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				Организационная мера+	СКЗИ + средства контроля подключения съёмных машинных носителей информации	—	Контроль использования внешних устройств и съёмных носителей. Шифрование
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации				Организационная мера+	СКЗИ	—	Шифрование
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съёмные машинные носители информации	+	+	+	—	СЗИ от НСД	**InfoWatch ARMA Endpoint**	—

ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съёмные машинные носители информации	+	+	+	—	Средства контроля подключения съёмных машинных носителей информации	—	Контроль использования внешних устройств и съёмных носителей
ЗНИ.6	Контроль ввода (вывода) информации на съёмные машинные носители информации			+	—	СЗИ от НСД	**InfoWatch ARMA Endpoint**	—
						Средства контроля подключения съёмных машинных носителей информации	—	Контроль использования внешних устройств и съёмных носителей
ЗНИ.7	Контроль подключения съёмных машинных носителей информации	+	+	+	Организацион-ная мера+	СЗИ от НСД	**InfoWatch ARMA Endpoint**	Контроль использования внешних устройств и съёмных носителей
						Средства контроля подключения съёмных машинных носителей информации	—	Контроль использования внешних устройств и съёмных носителей
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+	+	+	Организацион-ная мера+	СЗИ от НСД СКЗИ	—	—
V. Аудит безопасности (АУД)								
АУД.0	Регламентация правил и процедур аудита безопасности	+	+	+	Организацион-ная мера	—	—	—

АУД.1	Инвентаризация информационных ресурсов	+	+	+	Организацион-ная мера+	СЗИ от НСД	—	Инвентаризация используемого ПО, оборудования, внешних носителей
						Сканер безопасности	—	—
						МЭ	**InfoWatch ARMA Industrial Firewall**	—
АУД.2	Анализ уязвимостей и их устранение	+	+	+	—	Сканер безопасности	—	+ исследования и пен-тесты
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+	—	СОЕВ	—	—
АУД.4	Регистрация событий безопасности	+	+	+	—	МЭ СОВ	**InfoWatch ARMA Industrial Firewall**	—
						СЗИ от НСД	—	Любые системы мониторинга и защиты информации
АУД.4	Регистрация событий безопасности	+	+	+	—	СЗИ от НСД	—	Любые системы мониторинга и защиты информации
						SIEM	**InfoWatch ARMA Management Console**	Для сбора и регистрации событий из перечисленных систем
АУД.5	Контроль и анализ сетевого трафика			+	—	МЭ СОВ	**InfoWatch ARMA Industrial Firewall**	—
АУД.6	Защита информации о событиях безопасности	+	+	+	Организацион-ная мера+	Система мониторинга	—	Мониторинг действий сотрудников
АУД.7	Мониторинг безопасности	+	+	+	Организацион-ная мера+	СЗИ от НСД	—	—

АУД.7	Мониторинг безопасности	+	+	+	Организационная мера+	Сканер безопасности	—	Сканирование открытых портов, используемого ПО и приложений
						МЭ СОВ	**InfoWatch ARMA Industrial Firewall**	—
						Система мониторинга	—	Контроль над рабочим местом отдельного сотрудника
						SIEM	**InfoWatch ARMA Management Console**	—
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+	Организационная мера	—	—	—
АУД.9	Анализ действий отдельных пользователей			+	—	SIEM	**InfoWatch ARMA Management Console**	—
						Система мониторинга	—	Контроль над рабочим местом отдельного сотрудника
АУД.10	Проведение внутренних аудитов	+	+	+	Организационная мера	—	—	—
АУД.11	Проведение внешних аудитов				Организационная мера+	—	—	—
VI. Антивирусная защита (АВЗ)								
АВЗ.0	Регламентация правил и процедур антивирусной защиты	+	+	+	Организационная мера	—	—	—
АВЗ.1	Реализация антивирусной защиты	+	+	+	—	Средства антивирусной защиты	—	—

АВЗ.1	Реализация антивирусной защиты	+	+	+	—	СЗИ от НСД	**InfoWatch ARMA Industrial Firewall**	—
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+	+	+	—	Средства антивирусной защиты	—	—
						СЗИ от НСД	**InfoWatch ARMA Endpoint**	—
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов			+	—	СЗИ от НСД	**InfoWatch ARMA Endpoint**	—
						Средства антивирусной защиты	—	—
						Эмулятор среды функционирования ПО	—	—
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	—	Средства антивирусной защиты	—	—
						Эмулятор среды функционирования ПО	—	—
АВЗ.5	Использование средств антивирусной защиты различных производителей			+	Организационная мера	—	—	—

VII. Предотвращение вторжений (компьютерных атак) (СОВ)

СОВ.0	Регламентация правил и процедур предотвращения вторжений (компьютерных атак)		+	+	Организационная мера	—	—	—
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+	—	СОВ / СПВ (ФСТЭК) СОА (ФСБ)	**InfoWatch ARMA Industrial Firewall**	—

СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+	—	SIEM	**InfoWatch ARMA Management Console**	—
СОВ.2	Обновление базы решающих правил		+	+	—	СОВ / СПВ (ФСТЭК) СОА (ФСБ)	**InfoWatch ARMA Industrial Firewall**	—
						SIEM	**InfoWatch ARMA Management Console**	—

VIII. Обеспечение целостности (ОЦЛ)

ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	+	+	+	Организацион-ная мера	—	—	—
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+	—	СЗИ от НСД	**InfoWatch ARMA Endpoint**	Контроль целостности ПО рабочих станций и серверов
ОЦЛ.2	Контроль целостности информации				—	СЗИ от НСД	—	Контроль целостности на основе цифровых отпечатков
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			+	—	СЗИ от НСД	—	Точечный контроль сотрудников
						МЭ	**InfoWatch ARMA Industrial Firewall**	Для данных, вводимых в панели управления СЗИ, и контроль параметров промышленных протоколов
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+	—	СЗИ от НСД	—	Точечный контроль сотрудников
						МЭ	**InfoWatch ARMA Industrial Firewall**	Для данных, вводимых в панели управления СЗИ, и контроль параметров промышленных протоколов
						ППО	—	—

ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+	—	СЗИ от НСД	—	Точечный контроль сотрудников
						МЭ	**InfoWatch ARMA Industrial Firewall**	Для данных, вводимых в панели управления СЗИ, и контроль параметров промышленных протоколов
ОЦЛ.6	Обезличивание и (или) деидентификация информации				Организационная мера	ППО (СУБД)	—	—
IX. Обеспечение доступности (ОДТ)								
ОДТ.0	Регламентация правил и процедур обеспечения целостности	+	+	+	Организационная мера	—	—	—
ОДТ.1	Использование отказоустойчивых технических средств		+	+	Организационная мера+	—	—	ТС + ServiceDesk
ОДТ.2	Резервирование средств и систем		+	+	Организационная мера+	Кластеризация + резервирование каналов связи	—	—
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+	Организационная мера+	Системы мониторинга Service Desk	—	—
ОДТ.4	Резервное копирование информации	+	+	+	Организационная мера+	Backup / recovery	—	—
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+	Организационная мера+	Backup / recovery	—	—
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+	Организационная мера+	Backup / recovery	—	—
ОДТ.7	Кластеризация информационной (автоматизированной) системы				—	—	—	—

ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+	+	+	—	—	—	—
X. Защита технических средств и систем (ЗТС)								
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	+	+	+	Организационная мера	—	—	—
ЗТС.1	Защита информации от утечки по техническим каналам				Организационная мера+	СЗИ от УТК (генераторы и т. д.)	—	—
ЗТС.2	Организация контролируемой зоны	+	+	+	Организационная мера+	КИТСО	—	—
ЗТС.3	Управление физическим доступом	+	+	+	Организационная мера+	КИТСО	—	—
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр	+	+	+	Организационная мера+	КИТСО	—	—
ЗТС.5	Защита от внешних воздействий	+	+	+	Организационная мера+	КИТСО	—	—
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешённой к обработке информации				Организационная мера+	КИТСО	—	—
XI. Защита информационной (автоматизированной) системы и её компонентов (ЗИС)								
ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и её компонентов	+	+	+	Организационная мера	—	—	—

ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+	Организацион-ная мера+	СЗИ от НСД	—	—
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+	+	+	—	МЭ СОВ / СПВ	**InfoWatch ARMA Industrial Firewall**	—
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+	—	МЭ СОВ / СПВ	**InfoWatch ARMA Industrial Firewall**	—
ЗИС.4	Сегментирование информационной (автоматизированной) системы		+	+	—	МЭ	**InfoWatch ARMA Industrial Firewall**	—
ЗИС.5	Организация демилитаризованной зоны	+	+	+	—	МЭ	**InfoWatch ARMA Industrial Firewall**	—
ЗИС.6	Управление сетевыми потоками	+	+	+	—	МЭ	**InfoWatch ARMA Industrial Firewall**	—
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения («песочница»)				—	Эмулятор среды функционирова-ния ПО	—	—
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+	+	+	—	МЭ	**InfoWatch ARMA Industrial Firewall**	—
ЗИС.9	Создание гетерогенной среды				—	—	—	—
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем				—	СЗИ от НСД	—	ОС: Windows, Astra Linux
ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				—	МЭ	**InfoWatch ARMA Industrial Firewall**	—

ЗИС.12	Использование программного обеспечения, функционирующего в средах различных операционных систем				—	ОС СЗ среды виртуализации	—	—
ЗИС.13	Защита неизменяемых данных		+	+	—	СЗИ от НСД СКЗИ	**InfoWatch ARMA Endpoint**	—
ЗИС.14	Использование неперезаписываемых машинных носителей информации				Организационная мера, комплектование СВТ	—	—	—
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек				Организационная мера+	—	—	—
ЗИС.16	Защита от спама		+	+	—	Системы «Антиспам»	—	SPAM Filter
ЗИС.17	Защита информации от утечек				—	DLP	—	Контроль информационных потоков основных каналов передачи данных
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию				—	МЭ СОВ / СПВ	**InfoWatch ARMA Industrial Firewall**	—
						Средства антивирусной защиты	—	—
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию				—	Система мониторинга	—	Чёрные и белые списки
ЗИС.19	Защита информации при её передаче по каналам связи	+	+	+	—	СКЗИ (VPN)	—	Шифрование
ЗИС.20	Обеспечение доверенных канала, маршрута	+	+	+	—	СКЗИ (VPN)	—	—

ЗИС.21	Защита информации при её передаче по каналам связи	+	+	+	Организацион-ная мера+	ОС СКЗИ (VPN)	—	—	
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами				—	ОС СЗИ от НСД ППО	—	—	
ЗИС.23	Контроль использования мобильного кода				—	MDM	—	—	
						Специализиро-ванное ПО	—	—	
ЗИС.24	Контроль передачи речевой информации				Организацион-ная мера+	DLP	—	—	
						МЭ СОВ / СПВ	**InfoWatch ARMA Industrial Firewall**	—	
ЗИС.25	Контроль передачи видеоинформации				Организацион-ная мера+	МЭ СОВ / СПВ	**InfoWatch ARMA Industrial Firewall**	—	
ЗИС.26	Подтверждение происхождения источника информации				—	СКЗИ (VPN, ЭЦП)	—	—	
ЗИС.27	Обеспечение подлинности сетевых соединений		+	+	—	СКЗИ (VPN, ЭЦП)	—	—	
ЗИС.28	Исключение возможности отрицания отправки информации				—	СКЗИ (VPN, ЭЦП)	—	—	
ЗИС.28	Исключение возможности отрицания отправки информации				—	Система мониторинга	—	Проведение внутренней проверки	

ЗИС.29	Исключение возможности отрицания получения информации				—	СКЗИ (VPN, ЭЦП)	—	—
						Система мониторинга	—	Проведение внутренней проверки
ЗИС.30	Использование устройств терминального доступа				—	—	—	Контроль средств печати, терминальных устройств хранения и самонастраиваемых устройств
ЗИС.31	Защита от скрытых каналов передачи информации				—	СЗИ от НСД (в т. ч. создание замкнутой программной среды)	**InfoWatch ARMA Industrial Firewall**	Контроль передачи полезных данных внутри других данных (метаданные файловых форматов). Контроль передачи данных с использованием бинарных протоколов внутри стандартных протоколов (частично) + исследования
ЗИС.32	Защита беспроводных соединений	+	+	+	—	СКЗИ (VPN)	—	—
ЗИС.33	Исключение доступа через общие ресурсы	+	+	+	Организацион-ная мера+	СКЗИ (VPN)	—	—
						МЭ	**InfoWatch ARMA Industrial Firewall**	—
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDoS-атак)	+	+	+	—	Система защиты от сетевых атак	**InfoWatch ARMA Industrial Firewall**	—
ЗИС.35	Управление сетевыми соединениями	+	+	+	—	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)				—	ОС Специализи-рованное ПО + средства класте-ризации	—	—
ЗИС.38	Защита информации при использовании мобильных устройств	+	+	+	—	MDM	—	Контроль основных каналов передачи данных
						СКЗИ (VPN)	—	—
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+	+	+	Организацион-ная мера+	Системы защиты виртуализации	—	—
XII. Реагирование на компьютерные инциденты (ИНЦ)								
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	+	+	+	Организацион-ная мера	—	—	—
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+	—	Все виды СЗИ, МЭ	**InfoWatch ARMA Industrial Firewall**	—
						DLP	—	Событийная модель предоставления информации об инцидентах
						SIEM	**InfoWatch ARMA Management Console**	—
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+	—	Все виды СЗИ, МЭ, DLP	**InfoWatch ARMA Industrial Firewall**	Оповещение офицера безопасности об инциденте
						SIEM	**InfoWatch ARMA Management Console**	Оповещение офицера безопасности об инциденте

ИНЦ.3	Анализ компьютерных инцидентов	+	+	+	Организационная мера+	SIEM	**InfoWatch ARMA Management Console**	—
ИНЦ.4	Анализ компьютерных инцидентов	+	+	+	Организационная мера+	SIEM	**InfoWatch ARMA Management Console**	—
						Backup / recovery	—	—
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+	Организационная мера	—	—	—
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+	+	+	Организационная мера+	Все виды СЗИ	—	Организация структурированного хранения данных с ограничением доступа на основе ролевой модели
						SIEM	**InfoWatch ARMA Management Console**	—
						Средства в составе ГосСопка	—	—
XIII. Управление конфигурацией (УКФ)								
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	+	+	+	Организационная мера	—	—	—
УКФ.1	Идентификация объектов управления конфигурацией				—	ПО для реализации процессов SACM	—	—
УКФ.2	Управление изменениями	+	+	+	—	ПО для реализации процессов SACM	—	—

УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+	Организационная мера+	СЗИ от НСД (в т. ч. создание замкнутой программной среды)	**InfoWatch ARMA Endpoint**	—
УКФ.4	Контроль действий по внесению изменений				—	ПО для реализации процессов SACM	—	—
						СЗИ от НСД Средства мониторинга	—	—

XIV. Управление обновлениями программного обеспечения (ОПО)

ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+	+	+	Организационная мера	—	—	—
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+	Организационная мера+	СКЗИ (VPN, ЭЦП)	—	—
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+	Организационная мера+	ОС	—	—
						СЗИ от НСД	—	Контроль целостности
						СКЗИ (VPN, ЭЦП)	—	—
ОПО.3	Тестирование обновлений программного обеспечения	+	+	+	Организационная мера+	Стенд	—	Может использоваться для тестирования обновления на безопасность среды
ОПО.4	Установка обновлений программного обеспечения	+	+	+	—	ОС ППО	—	—

XV. Планирование мероприятий по обеспечению безопасности (ПЛН)

ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	+	+	+	Организационная мера	—	—	—
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+	+	+	Организационная мера	—	—	—
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+	+	+	Организационная мера+	Средства контроля эффективности защиты (защищённости)	—	—

XVI. Обеспечение действий в нештатных ситуациях (ДНС)

ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+	+	+	Организационная мера	—	—	—
ДНС.1	Разработка плана действий в нештатных ситуациях	+	+	+	Организационная мера	—	—	—
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+	+	+	Организационная мера	—	—	—
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций		+	+	Организационная мера+	Backup / recovery	—	—
						СКЗИ	—	Контроль целостности
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций		+	+	Организационная мера+	—	—	—

ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+		+	Организацион-ная мера	Backup / recovery	—	—
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+	+	+	Организацион-ная мера+	COB	**InfoWatch ARMA Industrial Firewall**	—
						SIEM	**InfoWatch ARMA Management Console**	—

XVII. Информирование и обучение персонала (ИПО)

ИПО.0	Регламентация правил и процедур информирования и обучения персонала	+	+	+	Организацион-ная мера	—	—	—
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+	Организацион-ная мера+	Интеграционные решения	—	Тестирование на основе подложных email и дальнейшее информирование о допущенных ошибках
ИПО.2	Обучение персонала правилам безопасной работы	+	+	+	Организацион-ная мера+	Интеграционные решения	—	Оповещение о необходимых мероприятиях и курсах
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы		+	+	Организацион-ная мера+	Интеграционные решения	—	Проведение демонстраций
ИПО.4	Контроль осведомлённости персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+	Организацион-ная 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.