Средства защиты информации, производимые и поставляемые АЛТЭКС-СОФТ для реализации базовых мер защиты информационных систем (ГИС и ИСПДн)

Условные обозначения:

сертифицированная платформа Microsoft -клиентские и серверные операционные систем, офисные пакеты, средства групповой работы, СУБД и др. программные продукты, имеющие встроенные механизмы защиты прошедшие сертификацию по требованиям ФСТЭК России (более 50 действующих Сертификатов). Применяются в качестве базовых СЗИ для реализации мер защиты ГИС 3 и 4 классов защиты, ИСПДн 3 и 4 уровней защищенности при отсутствии угроз 2-го типа и АС, в которых не предъявляются требования контроля НДВ СЗИ.

РОСА Кобальт - современная серверная и клиентская сертифицированная Linux операционная система, Сертифицирована на соответствие 5 классу СВТ, 4 уровень контроля отсутствия НДВ. Применяется в качестве базового СЗИ для реализации мер защиты в ГИС, ИСПДн и АС, всех уровней защищенности/ классов защиты, не обрабатывающих государственную тайну.

РОСА ХРОМ - современная серверная и клиентская сертифицированная Linux операционная система, Сертифицирована на соответствие 4 классу СВТ, 3 уровень контроля НДВ. Применяется в качестве базового СЗИ для реализации мер защиты в ГИС, ИСПДн и АС, всех уровней защищенности/ классов защиты, в том числе обрабатывающих государственную тайну не выше «секретно».

RedCheck - комплексное средство анализа защищенности (сканер безопасности). Сертифицирован на соответствие ТУ, 4 уровень контроля отсутствия НДВ. Реализует меры защиты в части контроля (анализа) защищенности информации (АНЗ) и контроля целостности (ОЦЛ), а также ряда «смежных» мер для информационных систем всех уровней защищенности/ классов защиты, не обрабатывающих государственную тайну.

UserGate Proxy&Firewall VPN GOST – программный комплекс, реализующий функции межсетевого экрана, системы обнаружения вторжений, средства защищенного доступа в сети общего пользования. Сертифицирован на соответствие: РД МЭ- 3 класс, документа «Требования к системам обнаружения вторжений» - по 4 классу защиты (ИТ.СОВ.С4.ПЗ), имеет оценочный уровень доверия ОУД3 (усиленный) в соответствии с требованиями руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», 4 уровень контроля отсутствия НДВ.

Acronis Backup & Recovery - система резервного копирования и аварийного восстановления рабочих станций и серверов. Сертифицирована на соответствие ТУ, 4 уровень контроля отсутствия НДВ. Реализует меры защиты в части обеспечения целостности (ОЦЛ, ЗСВ) информационных систем всех уровней/ классов защиты, не обрабатывающих государственную тайну.

DeviceLock DLP **DeviceLock** – программный комплекс для предотвращения неконтролируемых действий пользователей при обмене информацией через компьютерные порты, сменные носители, сетевые протоколы и коммуникационные приложения. Сертифицирован на соответствие 3Б и имеет оценочный уровень доверия ОУД2 в соответствии с требованиями руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», 4 уровень контроля отсутствия НДВ. Применяется для реализации группы мер защиты, связанных с контролем использованиям внешних и мобильных устройств, а также передачи информации во внешние системы, предназначен для информационных систем всех уровней/ классов защиты, не обрабатывающих государственную тайну.

АПК «ДИОД 0.1» **АПК «ДИОД 0.1» -** аппаратно-программный комплекс однонаправленной передачи данных, обеспечивает однонаправленность на физическом уровне. Реализует меры управления доступом (УПД) и защиты систем связи и передачи данных. (ЗИС). Сертифицирован на соответствие ТУ, 3 уровень контроля отсутствия НДВ. Может применяться для защиты государственной тайны не выше «секретно».

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)						
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Microsoft Certified POCA Кобальт		POCA Кобальт		Использованием встроенных механизмов аутентификации и защиты сертифицированных ОС Microsoft и POCA. Выполняется с помощью установки соответствующих параметров безопасности механизмов «Идентификации и аутентификации» при настройке операционной системы на сертифицированную конфигурацию для пользователей домена (для сетей ЭВМ) и локальных пользователей (на уровне автономных рабочих мест)..В случае использования других элементов общего программного обеспечения (SQL Server, Exchange Server и др.) дополнительно используются их встроенные механизмы «Идентификация и др.)
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных					
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов					
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компромета-					

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	ции средств аутентификации					
ИАФ.5	Защита обратной связи при вводе аутентификационной информации					
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)					
ИАФ.7 (только для ГИС)	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа					
II. Управление доступом субъектов доступа к объектам доступа (УПД)						
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей					Реализуется штатными средствами контроля доступа ОС: Сертифицированные ОС Windows и РОСА «Кобальт» - дискреционный доступ. РОСА «Хром» -мандатный доступ.
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа					
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами,					Фильтрация и маршрутизация обеспечивается функциями межсетевого экрана UserGate. Однонаправленность обеспечивается оптической развязкой АПК «ДИОД 0.1»

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	сегментами информационной системы, а также между информационными системами					
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы					Реализуется средствами разграничения доступа ОС,
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы					
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)					
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации					Необязательная мера. Реализуется как правило функциями прикладного ПО
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему					
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя					Штатные механизмы контроля доступа сертифицированных ОС

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Microsoft Certified	Microsoft Certified	POCA Кобальт		
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации					
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки					
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	UserGate Proxy & Firewall				Реализуется при помощи криптографической аутентификации на основе сертификатов X.509 и организацией виртуальных частных сетей (VPN) для удаленного защищенного доступа через открытые каналы Интернета к серверам баз данных, FTP, почтовым серверам и пр.
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+	Организационные меры
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	DeviceLock DLP				Механизмы контроля за мобильными устройствами сертифицированного ПК DeviceLock
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внеш-	UserGate Proxy & Firewall				Средства управления доступом UserGate

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	ние информационные системы)					
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+	Использование решений партнеров (Соболь, Аккорд и пр.)
III. Ограничение программной среды (ОПС)						
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				POCA Кобальт	Применение политик ограниченного использования программ сертифицированными ОС
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			RedCheck POCA Кобальт		Применение «политик ограниченного использования программ» сертифицированными ОС. Контроль за установкой ПО осуществляется средствами инвентаризации RedCheck
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	RedCheck Microsoft Certified				
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов					Реализуется механизмами и политиками удаления файлов сертифицированных ОС
IV. Защита машинных носителей информации (ЗНИ)						
ЗНИ.1	Учет машинных носителей ин-	+	+	+	+	Организационные меры

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	формации					
ЗНИ.2	Управление доступом к машинным носителям информации	DeviceLock DLP				Механизмы контроля за сменными носителями сертифицированного ПК DeviceLock
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны					Организационные меры
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах	DeviceLock DLP				Механизмы контроля за сменными носителями и портами сертифицированного ПК DeviceLock
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации					
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации					
ЗНИ.7	Контроль подключения машинных носителей информации					
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	blancco				Полное стирание достигается перезаписью информационных объектов, включая перераспределённые сектора, повреждённые сектора и скрытые области, специальной последовательностью байт.
V. Регистрация событий безопасности (РСБ)						
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения					Механизмы аудита сертифицированных ОС

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации					
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения					
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти					
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них					
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе					
РСБ.7	Защита информации о событиях безопасности					
РСБ.8 (только для ГИС)	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе					
VI. Антивирусная защита (АВЗ)						
АВЗ.1	Реализация антивирусной защиты	+	+	+	+	Сертифицированные антивирусные решения партнеров

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+	(Kaspersky, Dr.Web).
VII. Обнаружение вторжений (СОВ)						
СОВ.1	Обнаружение вторжений	UserGate Proxy & Firewall				Встроенный модуль IDS, сертифицирован на соответствие "Требованиям к системам обнаружения вторжений" (ИТ.СОВ.С4.ПЗ),– по 4 классу защиты.
СОВ.2	Обновление базы решающих правил					
VIII. Контроль (анализ) защищенности информации (АН3)						
АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		RedCheck			Базовые функции RedCheck: - аудит уязвимостей и критичных обновлений; - аудит конфигураций безопасности; - оценка соответствия политикам и стандартам; - инвентаризация программного и аппаратно-программного; - анализ сетевой активности; - проверка сложности паролей.
АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	RedCheck				
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		RedCheck			
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации					
АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения			POCA Кобальт		

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	доступом, полномочий пользователей в информационной системе					
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)						
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			RedCheck		Базовая функция контроля целостности на файловом уровне с использованием встроенного сертифицированного СЗИ «ФИКС».
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы					
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	Acronis				Базовые функции резервирования и восстановления данных.
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+	Использование решений партнеров (Kaspersky, Entensys и пр.)
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче	DeviceLock DLP				Базовые функции и использование модулей ContentLock, NetworkLock

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы					
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				+	Реализация на уровне прикладного программного обеспечения
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему					
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	DeviceLock DLP				Базовые функции и использование модуля NetworkLock
X. Обеспечение доступности информации (ОДТ)						
ОДТ.1	Использование отказоустойчивых технических средств				+	Организационно-технические меры
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				+	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование			+	+	
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители			Acronis		Базовые функции резервного копирования и восстановления

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	информации					
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала					
ОДТ.6 (только для ГИС)	Кластеризация информационной системы и (или) ее сегментов					
ОДТ.7 (только для ГИС)	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации			+	+	Организационно-технические меры
XI. Защита среды виртуализации (ЗСВ)						
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации			+	+	Средства безопасности Hyper-V из состава сертифицированных Microsoft Windows Server. Сертифицированные решения партнеров (VMware vSphere, vGate)
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин			+	+	
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре			+	+	
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами			+	+	

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры					
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией					Необязательная мера
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+	Организационная мера
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+	
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	Acronis				Базовые функции резервного копирования и восстановления
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+	Сертифицированные антивирусные решения партнеров (Kaspersky, Dr.Web).
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей		+ (только для ИСПДн)	+	+	Организационная мера
XII. Защита технических средств (ЗТС)						
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по					Организационные меры

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	техническим каналам					
ЗТС.2 (только для ГИС)	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	+	+	+	+	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	+	+	+	+	
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+	
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				+ (только для ГИС)	

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)						
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы			+ (только для ГИС)	+	Организационные меры
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритет ом со стороны процессов с низким приоритетом					
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи					Организация VPN с использованием ПК UserGate и встроенного СКЗИ КриптоПро CSP
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)					
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно,	+	+	+	+	Организационные меры

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	и оповещение пользователей об активации таких устройств					
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами					
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода			+	+	Организационные меры
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи			+	+	Организационные меры
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей ви-			+	+	

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	деоинформации					
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам			РОСА Кобальт		Сертифицированные ОС в роли DNS-серверов
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов					
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю			+	+	Использование в составе сертифицированных ОС СКЗИ для реализации электронной подписи (КриптоПро CSP и др.)
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя			+	+	
ЗИС.14	Использование устройств терминального доступа для обработки информации			РОСА Кобальт		Использование сертифицированных серверных ОС в роли RDS и клиентских ОС на терминальных клиентах
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации			+	+	Организационно-технические меры
ЗИС.16	Выявление, анализ и блокирование в информационной си-					Антивирусные средства, возможно использование ПК

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	стеме скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов					RedCheck, как средства диагностики открытых портов
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			UserGate Proxy & Firewall АПК «ДИОД 0.1»		Разделение информационных систем на логическом и физическом уровнях
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения					Организационно-техническая мера реализуется на уровне прикладного ПО.
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			РОСА Кобальт		Обеспечивается штатными механизмами изоляции процессов сертифицированных ОС
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+	Организационно-техническая мера
ЗИС.21 (только для ГИС)	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через регистры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы				АПК «ДИОД 0.1»	Обеспечивается аппаратной реализацией информационных систем

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
ЗИС.22 (только для ГИС)	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы			+	+	Обеспечивается аппаратной реализацией информационных систем и использованием специальных СЗИ
ЗИС.23 (только для ГИС)	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями			UserGate Proxy & Firewall		Базовые механизмы управления потоками (фильтрация, маршрутизация)
ЗИС.24 (только для ГИС)	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения					
ЗИС.25 (только для ГИС)	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)					Организационно-технические меры
ЗИС.26 (только для ГИС)	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем					
ЗИС.27 (только для ГИС)	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз					

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	безопасности информации					
ЗИС.28 (только для ГИС)	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы					
ЗИС.29 (только для ГИС)	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы					
ЗИС.30 (только для ГИС)	Защита мобильных технических средств, применяемых в информационной системе		+	+	+	
XIV. Выявление инцидентов и реагирование на них (ИНЦ)						
ИНЦ.1 (только для ИСПДн)	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+	Организационные меры
ИНЦ.2 (только для ИСПДн)	Обнаружение, идентификация и регистрация инцидентов			+	+	
ИНЦ.3	Своевременное информи-					Использование ПК DeviceLock,

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
(только для ИСПДн)	рование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			POCA Кобальт UserGate Proxy & Firewall DeviceLock DLP		для анализа инцидентов, связанных с утечками информации, средств регистрации ОС, МЭ и других программ – для других случаев
ИНЦ.4 (только для ИСПДн)	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий					
ИНЦ.5 (только для ИСПДн)	Принятие мер по устранению последствий инцидентов					
ИНЦ.6 (только для ИСПДн)	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+	Организационные меры
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)						
УКФ.1 (только для ИСПДн)	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+	Организационно- технические меры
УКФ.2 (только для ИСПДн)	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		RedCheck			Реализуется функциями аудит конфигураций ПК RedCheck
УКФ.3 (только для ИСПДн)	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных дан-		+	+	+	Организационно- технические меры

Условное обозначение меры	Меры защиты информации в информационных системах	Уровни/ классы защищенности информационных систем				Описание механизмов защиты
		4	3	2	1	
	ных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных					
УКФ.4 (только для ИСПДн)	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		RedCheck			Реализуется функциями аудит конфигураций совместно с построением отчётов ПК RedCheck

Узнать больше о заявленных (сертифицированных) функциональных возможностях можно в разделе нашего сайта «Задания по безопасности и технические условия» или обратившись в службу технической поддержки.