# СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ПРОИЗВОДИМЫЕ И ПОСТАВЛЯЕМЫЕ «АЛТЭКС-СОФТ» ДЛЯ РЕАЛИЗАЦИИ МЕР ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ (ГИС И ИСПДН)

**Условные обозначения**

Microsoft CERTIFIED

Сертифицированная платформа Microsoft - клиентские и серверные операционные системы, офисные пакеты, средства групповой работы, СУБД и другие 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 ГИС3 и 4 классов защиты, ИСПДн3 и 4 уровней защищенности при отсутствии угроз 2-го типа и АС, в которых не предъявляются требования контроля НДВ СЗИ.

RED Check

RedCheck - комплексное средство анализа защищенности (сканер безопасности). Сертифицирован на соответствие ТУ, 4 уровень доверия. 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.

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point Security Gateway R77.30 - сертифицированный ФСТЭК России программно-аппаратный (программный) комплекс Шлюз безопасности для применения на физической или логической границе (периметре) информационных систем для реализации функций межсетевого экрана и системы обнаружения вторжений.

DeviceLock

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». Применяется для реализации группы мер защиты, связанных с контролем использования внешних и мобильных устройств, а также передачи информации во внешние системы, предназначен для информационных систем всех уровней/классов защиты, не обрабатывающих государственную тайну.

vmware vSOM

VMwarevSOM – масштабируемая платформа для виртуализации ЦОД, отдельных серверов и рабочих станций с возможностью централизованного управления и мониторинга. Сертифицирован на соответствие ТУ, реализует меры защиты в части защиты среды виртуализации, в частности 3СВ.1, 3СВ.2, 3СВ.3, 3СВ.6, 3СВ.7, 3СВ.8, 3СВ.10. Программный комплекс может использоваться в составе АС до класса защищенности 1Г, ИСПДн и ГИС 3, 4 уровней (классов) защищенности.

Astra Linux Special Edition – Сертифицированная операционная система специального назначения, предназначеная для создания на ее основе автоматизированных систем в защищенном исполнении, обрабатывающих информацию со степенью секретности "совершенно секретно" включительно.

Альт Линукс СПТ 7.0 — унифицированный дистрибутив для серверов, рабочих станций и тонких клиентов со встроенными программными средствами защиты информации, сертифицированный ФСТЭК России. Соответствует требованиям руководящих документов "Средства вычислительной техники. Защищает от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации" — по 4 классу защищенности; "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей" — по 3 уровню контроля и технических условий при выполнении указаний по эксплуатации, приведенных в формуляре КШДС.10514-01 30.01. Может быть использован для построения автоматизированных систем по класс 1В включительно и информационных систем персональных данных (ИСПДн) по класс 1К включительно.

Операционные системы семейства РОСА предназначены для организации вычислительного процесса в защищенных автоматизированных системах (АС) различного назначения на современных 32/64-разрядных аппаратных платформах с архитектурой x86_64 на базе процессоров Intel и AMD. Сертифицированные по требованиям безопасности (ФСТЭК России) операционные системы РОСА "Хром" и "Кобальт" пригодны для использования в органах военного управления, министерствах и ведомствах, органах исполнительной власти, а также на предприятиях промышленности, работающих с информацией ограниченного пользования, включая государственную тайну.

StaffCop Enterprise – информационно-аналитическая система для контроля действий сотрудников, потоков информации и событий системы. StaffCop фиксирует все события, каналы движения информации и файлов внутри компании и их передачу за пределы. Позволяет анализировать эффективность деятельности сотрудников, получить реальный KPI, а также обеспечить контроль и защиту важной информации, расследовать инциденты, выявлять инсайдеров и злоумышленников.

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| **Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | | | | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | Microsoft CERTIFIED | | | | Использованием встроенных механизмов аутентификации и защиты сертифицированных ОС. 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 | Microsoft CERTIFIED | | | | |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации 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 | 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 | | | | | |
| | **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, 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 | | | | | |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | Microsoft CERTIFIED | | ASTRALINUX, ROSA, base alt, СПТ | | |
| 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 информационной системы | ROSA, ASTRALINUX | | | | Штатные механизмы контроля доступа сертифицированных ОС |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | Microsoft CERTIFIED | | ASTRALINUX, ROSA, base alt, СПТ | | |
| 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 | STAFFCOP | | | | |
| 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 | | | | Механизмы контроля за мобильными устройствами сертифицированного ПК DeviceLock |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + | + | + | + | |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | | | + | + | Использование решений партнеров (Соболь, Аккорд и пр.) |
| | **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 | ROSA, ASTRALINUX special edition | | | | 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 | | | STAFFCOP | | Применение «политик ограниченного использования программ» сертифицированными ОС и средствами Staffcop. Контроль за установкой ПО также осуществляется средствами инвентаризации |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | STAFFCOP, Microsoft CERTIFIED | | | | |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов | ASTRALINUX special edition, ROSA, base alt | | | | Реализуется механизмами и политиками удаления файлов сертифицированных ОС |
| | **Защита машинных носителей информации (ЗНИ)** | | | | | |
| ЗНИ.1 | Учет машинных носителей информации | + | + | + | + | Организационные меры |
| ЗНИ.2 | Управление доступом к машинным носителям информации | DeviceLock | | | | 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 | STAFFCOP, DeviceLock | | | | Механизмы контроля за сменными носителями и портами сертифицированного ПК DeviceLock |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации | STAFFCOP DeviceLock | | | | |
| 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) | | + | + | + | |
| | **Регистрация событий безопасности (РСБ)** | | | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | STAFFCOP Microsoft CERTIFIED | | STAFFCOP ROSA ASTRALINUX special edition base alt СПТ | | Механизмы аудита сертифицированных ОС |
| 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 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе | | | | | |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| **Антивирусная защита (АВЗ)** | | | | | | |
| АВЗ.1 | Реализация антивирусной защиты | + | + | + | + | Сертифицированные антивирусные решения партнеров (Kaspersky, Dr.Web). |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | | | | | |
| **Обнаружение вторжений (СОВ)** | | | | | | |
| СОВ.1 | Обнаружение вторжений | Check Point SOFTWARE TECHNOLOGIES LTD. | | | | |
| СОВ.2 | Обновление базы решающих правил | | | | | |
| **Контроль (анализ) защищенности информации (АНЗ)** | | | | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | | RED Check | | | Базовые функции RedCheck:<br>- аудит уязвимостей и критичных обновлений;<br>- аудит конфигураций безопасности;<br>- оценка соответствия политикам и стандартам;<br>- инвентаризация программного и аппаратно-программного обеспечения;<br>- анализ сетевой активности;<br>- проверка сложности паролей. |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | RED Check | | | | |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | | RED Check | | | |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | | | | | |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе | Microsoft CERTIFIED | ASTRALINUX special edition; ROSA; base alt; CIIT | | | |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| **Обеспечение целостности информационной системы и информации (ОЦЛ)** | | | | | | |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | | | RED Check | | 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 | | | | | 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 информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы | | | STAFFCOP DeviceLock | | Базовые функции и использование модулей ContentLock, NetworkLock |
| 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 | | Базовые функции и использование модулей ContentLock, NetworkLock |
| **Обеспечение доступности информации (ОДТ)** | | | | | | |
| ОДТ.1 | Использование отказоустойчивых технических средств | | | | + | Организационно-технические меры |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| 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 информации | | | | | Базовые функции резервного копирования и восстановления |
| 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 |
| | **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 средства виртуализации VMware |
| 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 виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры | | | + | + | Базовые функции резервного копирования и восстановления |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| 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 | vmware vSOM | | + | + | Организационная мера |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | | | + | + | Базовые функции резервного копирования и восстановления |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | | | + | + | |
| 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 | vmware vSOM | | + | + | Организационная мера |
| | **Защита технических средств (ЗТС)** | | | | | |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам | | | | | Организационные меры |
| 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 | | + | + | + | |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| 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) | |

**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 приоритетом 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 | | + | + | + | |
| 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, 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 | | | | | |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| 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 | | | + | + | |
| 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 | | | + | + | |
| 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 видеоинформации | | | + | + | |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам | Check Point SOFTWARE TECHNOLOGIES LTD. | | Check Point SOFTWARE TECHNOLOGIES LTD.<br>ASTRALINUX special edition<br>ROSA base alt СПТ | | 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 | STAFFCOP | | | | |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя | STAFFCOP | | | | |
| ЗИС.14 | Использование устройств терминального доступа для обработки информации | | | ROSA base alt СПТ | | Использование сертифицированных серверных ОС в роли RDS и клиентских ОС на терминальных клиентах |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| 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 системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов | | | | | Антивирусные средства, возможно использование ПК RedCheck, как средства диагностики открытых портов |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | Check Point SOFTWARE TECHNOLOGIES LTD. | | | | 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 | | | ROSA ASTRALINUX special edition | | Обеспечивается штатными механизмами изоляции процессов сертифицированных ОС |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | | | | | |
| ЗИС.21 (только для ГИС) | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы | | | | + | Обеспечивается аппаратной реализацией информационных систем |
| ЗИС.22 (только для ГИС) | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы | Check Point SOFTWARE TECHNOLOGIES LTD. | | | | 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 | Check Point SOFTWARE TECHNOLOGIES LTD. | | | | |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| ЗИС.24 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения | | | + | + | |
| ЗИС.25 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) | | | | | Организационно-технические меры |
| ЗИС.26 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем | | | | | |
| ЗИС.27 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации | | | | | |
| ЗИС.28 | 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 | 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 | Защита мобильных технических средств, применяемых в информационной системе | | + | + | + | |
| **Выявление инцидентов и реагирование на них (ИНЦ)** | | | | | | |
| ИНЦ.1 (только для ИСПДн) | Определение лиц, ответственных за выявление инцидентов и реагирование на них | | | | | Организационные меры |

| Условное обозначение меры | Меры защиты информации в информационных системах | Уровни/ классы защищенности | | | | Описание механизмов защиты |
|---|---|---|---|---|---|---|
| | | 4 (ИСПДн) | 3 | 2 | 1 | |
| ИНЦ.2 (только для ИСПДн) | Обнаружение, идентификация и регистрация инцидентов | | | | | Организационные меры |
| ИНЦ.3 (только для ИСПДн) | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами | | | ROSA, Microsoft CERTIFIED, DeviceLock, STAFF-COP | | Использование ПК DeviceLock, 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 |
| **Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)** | | | | | | |
| УКФ.1 (только для ИСПДн) | Определение лиц, которым разрешены действияпо 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 | | RED Check | | | 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 персональныхданных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных | | + | + | + | Организационно-технические меры |
| УКФ.4 (только для ИСПДн) | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных | | RED Check | | | 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.