МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И СВЯЗИ КУЗБАССА (МИНЦИФРА КУЗБАССА)

ПРИКАЗ

от «13» апреля 2023 г. № 32 - п
г. Кемерово

Об утверждении инструкции по настройке автоматизированных рабочих мест с установленной операционной системой специального назначения Astra Linux Special Edition (Воронеж, Смоленск) для работы в государственных информационных системах Кемеровской области - Кузбасса

В целях выполнения требований приказа № 17 от 11.02.2013 Федеральной службы по техническому и экспортному контролю «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» п р и к а з ы в а ю:

1. Утвердить прилагаемую Инструкцию по настройке автоматизированных рабочих мест с установленной операционной системой специального назначения Astra Linux Special Edition (Воронеж, Смоленск) для работы в государственных информационных системах Кемеровской области - Кузбасса.

2. Отделу информационной безопасности управления информационной безопасности и связи Министерства цифрового развития и связи Кузбасса (Фомин С.С.), обеспечить контроль исполнения Инструкции по настройке автоматизированных рабочих мест с установленной операционной системой специального назначения Astra Linux Special Edition (Воронеж, Смоленск).

3. Государственному казенному учреждению «Центр информационных технологий Кузбасса» (Матвеев А.И.) использовать Инструкцию по настройке автоматизированных рабочих мест с установленной операционной системой специального назначения Astra Linux Special Edition (Воронеж, Смоленск) при подготовке автоматизированных рабочих мест.

4. Государственному автономному учреждению «Уполномоченный многофункциональный центр предоставления государственных и муниципальных услуг на территории Кузбасса» (Прозоров С.С.) использовать Инструкцию по настройке автоматизированных рабочих мест с установленной операционной системой специального назначения Astra Linux Special Edition (Воронеж, Смоленск) при подготовке автоматизированных рабочих мест.

5. Контроль за исполнением настоящего приказа оставляю за собой.

6. Настоящий приказ вступает в силу со дня подписания.

Министр М.В. Садиков

УТВЕРЖДЕНА
приказом Министерства цифрового
развития и связи Кузбасса
от 13 апреля 2023 г. № 32 - п

Инструкция
по настройке автоматизированных рабочих мест с установленной операционной системой специального назначения Astra Linux Special Edition (Воронеж) для работы в государственных информационных системах Кемеровкой области - Кузбасса

Настройка политики пароля

Длина и алфавит:

1. В файле **/etc/pam.d/common-password**, в строке ***password requisite pam cracklib.so*** установить значение ***minlen=8*** и добавить параметры ***dcredit=-1, ucredit=-1 u lcredit=-1*** (minlen – длина пароля, последние 3 параметра отвечают за алфавит (количество строчных, заглавных и цифр в пароле));

2. Количество дней между сменами пароля, попыток и время блокировки в файле /etc/login.defs:

- *# Количество дней между сменами пароля (дней)*

PASS_MAX_DAYS 90;

- *# Количество неуспешных попыток до блокировки*

LOGIN_RETRIES 6;

- *# Период блокировки в секундах после неудачных попыток (в секундах)*

LOGIN_TIMEOUT 1800.

Опционально:

1. Запрет повторного использования паролей:

- В файле **/etc/pam.d/common-password**, в строке «**...pam_unix.so**» добавить параметр **remember=x**, где x – число последних используемых паролей;

- Постоянный запрос пароля для команды sudo: в терминале ввести команду **sudo visudo,** в открывшемся файле добавляем строку **«Defaults timestamp_timeout=0»**.

2. Блокирование сеанса по времени не активности пользователя:

- в терминале запустить программу **sudo fly-admin-theme**;
- затем перейти в категорию «Блокировка»;
- Убедиться, что стоит галка «Блокировать экран»;
- Выставить в поле «После бездействия» - 15 минут.

Таблица №1
Реализация мер защиты информации
в соответствии с
приказом ФСТЭК России №17 от 11.02.2013
средствами операционной системы
специального назначения
Astra Linux Special Edition

Меры защиты информации в информационных системах		Классы защищенности ГИС		Средства реализации	Способ реализации меры защиты с использованием штатных средств Astra Linux	Компоненты Astra Linux	Эксплуатационная документация и справочная информация по функционированию и настройке штатных средств защиты информации Astra Linux
Код	Меры защиты информации	К3	К2				
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)							
1. ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+ 1а, 2а, 3	Средства Astra Linux + Организационные мероприятия + ОРД + СДЗ, токены	Идентификация и аутентификация пользователей осуществляется локально (по PAM) или централизованно с помощью организации единого пространства пользователей (ЕПП), в основу которого положен доменный принцип построения сети с использованием сетевого протокола сквозной доверенной аутентификации. При необходимости применения многофакторной аутентификации, ее использование обеспечивается совместным применением средств идентификации и аутентификации Astra Linux, средств доверенной загрузки и устройств аутентификации (например, USB-токенов).	Локальная идентификация и аутентификация (PAM), Сквозная аутентификация (ЕПП), Средства поддержки двухфакторной аутентификации	ОП: п.4.1.2 "Идентификация и аутентификация", п.4.1.3 "Организация ЕПП" РА.1: п.8 "Средства организации ЕПП", п.11.6 "Рабочий стол Fly", п.18 "Поддержка средств двухфакторной аутентификации" РКС3.1: п.2 "Идентификация и аутентификация" https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) https://wiki.astralinux.ru/x/RIImAg (Samba AD и Windows AD)

								https://wiki.astralinux.ru/x/XIV0Ag (СКЗИ) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
2.	ИАФ. 2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	Средства Astra Linux + ОРД	Идентификация устройств осуществляется по логическим именам, по комбинации имени, логического, физического адресов, по информации об устройстве локально или централизованно с использованием сетевого протокола сквозной доверенной аутентификации. Перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации, регламентируется ОРД. Аутентификация устройств реализуется средствами Astra Linux с использованием сетевого протокола сквозной доверенной аутентификации.	Идентификация устройств (ядро, parsec, dev), идентификация и аутентификация компьютеров в ЕПП (ALD, FreeIPA), сетевая идентификация компьютеров по именам и адресам, регистрация устройств локально (fly-admin-smc) и централизованно (FreeIPA, ALD), Защищенный комплекс программ печати и маркировки документов (cups)	РА.1: п.12.4 Настройка принтера и управления печатью, п.17 "Средства разграничения доступа к подключаемым носителям" РКСЗ.1: п.13 "Контроль подключения съемных машинных носителей информации" https://wiki.astralinux.ru/x/HAKtAg (Съемные носители в Astra Linux) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
3.	ИАФ. 3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+ 1а, 2а	+ 1а, 2а	Средства Astra Linux + Организационные мероприятия + ОРД	Управление идентификаторами пользователей (присвоение и блокирование идентификаторов, а также ограничение срока действия идентификаторов (учетных записей) осуществляется администратором локально или централизованно с помощью инструментов управления политикой безопасности. Управление идентификаторами устройств осуществляется администратором локально с помощью инструментов управления политикой безопасности или централизованно с использованием средств управления доменом.	Управление локальными пользователями (fly-admin-smc). Управление доменным пользователями (FreeIPA,ALD). Управление устройствами локально (fly-admin-smc) и в домене (FreeIPA,ALD)	РА.1: п.8 "Средства организации ЕПП", п.11.6 "Рабочий стол Fly" https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) https://wiki.astralinux.ru/x/RIImAg (Samba AD и Windows AD) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc

4.	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	+ 1б	+ 1в	Средства Astra Linux + Организационные мероприятия + ОРД При необходимости: СДЗ, токены	Управление средствами аутентификации осуществляется администратором локально или централизованно с помощью инструментов управления политикой безопасности. Для защиты аутентификационной информации в Astra Linux по умолчанию используются отечественные алгоритмы по ГОСТ 28147-89 и ГОСТ Р 34.11-2012 При необходимости применения многофакторной аутентификации, управление токенами производится с использованием средств поддержки двухфакторной аутентификации	Управление локальными пользователями (fly-admin-smc). Управление доменным пользователями (FreeIPA,ALD) Дополнительно: средства поддержки двухфакторной аутентификации	РА.1: п.8 "Средства организации ЕПП", п.11.6 "Рабочий стол Fly", п.18 "Поддержка средств двухфакторной аутентификации" https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) https://wiki.astralinux.ru/x/RIImAg (Samba AD и Windows AD) https://wiki.astralinux.ru/x/XIV0Ag (СКЗИ) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
5.	ИАФ. 5	Защита обратной связи при вводе аутентификационной информации	+	+	Средства Astra Linux	Защита обратной связи при вводе аутентификационной информации обеспечивается исключением отображения действительного значения аутентификационной информации при ее вводе пользователем в диалоговом интерфейсе средствами Astra Linux по умолчанию.	Защищённая графическая подсистема (fly-admin-dm, fly-dm, fly-qdm)	РП: п.3.2 "Графический вход в систему" Справка Astra Linux по утилитам настройки графического входа в систему fly-admin-dm, запуска серверной части системы fly-dm и поддержки графического интерфейса fly-qdm
6.	ИАФ. 6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	Средства Astra Linux + Организационные мероприятия + ОРД При необходимости: СДЗ, токены	Идентификация и аутентификация внешних пользователей осуществляется локально или централизованно с помощью организации единого пространства пользователей. При необходимости применения многофакторной аутентификации, ее использование обеспечивается совместным применением средств идентификации и аутентификации	Локальная идентификация и аутентификация (PAM), Сквозная аутентификация (ЕПП) Дополнительно: Средства поддержки двухфакторной аутентификации	ОП: п.4.1.2 "Идентификация и аутентификация", п.4.1.3 "Организация ЕПП" РА.1: п.8 "Средства организации ЕПП", п.11.6 "Рабочий стол Fly", п.18 "Поддержка средств двухфакторной аутентификации" РКСЗ.1: п.2

						Astra Linux, средств доверенной загрузки и устройств аутентификации (например, USB-токенов).		"Идентификация и аутентификация" https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) https://wiki.astralinux.ru/x/RIImAg (Samba AD и Windows AD) https://wiki.astralinux.ru/x/XIV0Ag (СКЗИ) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
7.	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			Средства Astra Linux	Идентификация всех объектов и устройств и применение результатов идентификации производится Astra Linux по умолчанию в том числе при реализации механизмов управления доступом, контроля целостности, резервного копирования и регистрации событий безопасности, связанных с этими объектами доступа. Аутентификация запускаемых и исполняемых модулей реализуется с использованием механизма контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнения (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")) . Аутентификация объектов файловой системы, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов	Контроль исполняемых файлов (ЗПС) Контроль расширенных атрибутов (ЗПС)	ОП: п.4.1.9 "Контроль целостности", п.4.1.10.1 "Замкнутая программная среда", п.4.1.10.2 "Системные ограничения и блокировки" РКСЗ.1: п.2 "Идентификация и аутентификация", п.16.1 "Замкнутая программная среда"

						доступа реализуется с использованием механизма контроля целостности файлов при их открытии на основе ЭП в расширенных атрибутах файловой системы (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")) .		
II. Управление доступом субъектов доступа к объектам доступа (УПД)								
1.	УПД. 1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+ 1,2	+ 1, 2, 3а	Средства Astra Linux + ОРД	Управление учетными записями пользователей (заведение, активация, блокирование и уничтожение) осуществляется администратором локально или централизованно с помощью инструментов управления политикой безопасности.	Управление локальными пользователями (fly-admin-smc), Управление доменным пользователями (FreeIPA, ALD)	РА.1: п.3.3 "Управление пользователями", п.8 "Средства организации ЕПП", п.11.6 "Рабочий стол Fly" https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) https://wiki.astralinux.ru/x/RIImAg (Samba AD и Windows AD) https://wiki.astralinux.ru/x/R4AS (ALD) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
2.	УПД. 2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной	+ 1, 2, 3	+ 1, 2, 3	Средства Astra Linux + ОРД	Монитор обращений из состава Astra Linux предусматривает дискреционное, мандатное (мандатное управление доступом доступно только для уровня защищенности Astra Linux	Дискреционное управление доступом, Управление полномочиями (привилегиями) локальных пользователей (fly-admin-smc), управление	РКСЗ.1: п.3 "Дискреционное управление доступом", п.4 "Мандатное управление доступом и мандатный контроль

		метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа				"Максимальный" ("Смоленск")) и ролевое управление доступом, а также реализацию мандатного контроля целостности (режим МКЦ доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")). Решение о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение, запись, исполнение), мандатного контекста безопасности пользователя и классификационной метки объекта. Управление доступом осуществляется применительно ко всем объектам, включая объекты файловой системы, базы данных, процессам и устройствам. Разделение полномочий (ролей) пользователей, назначение минимально необходимых прав и привилегий осуществляется администратором локально или централизованно с помощью инструментов управления политикой безопасности в соответствии с организационно-распорядительной документацией.	полномочиями (привилегиями/ролями) доменных пользователей (ALD/ FreeIPA) Дополнительно: мандатное управление доступом, МКЦ, управление доступом в БД	целостности" РА.2 ОП: п.4.1.4 "Дискреционное управление доступом", п.4.1.5 "Мандатное управление доступом и контроль целостности", п.4.1.17 "Обеспечение доступа к БД"
3.	УПД. 3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационным и потоками между устройствами,		+	МЭ или средства однонаправленной передачи, Средства Astra Linux, ОРД.	Управление информационными потоками осуществляется с использованием встроенного в ядро Astra Linux фильтра сетевых пакетов (netfilter) и монитора обращений. Управление правилами осуществляется администратором с использованием средств управления встроенным фильтром (iptables). Правила (или цепочки) фильтрации выполняются в соответствии с атрибутами отправителя и получателя	Средства межсетевого экранирования (astra-ufw-control)	РКСЗ.1: п.11 "Фильтрация сетевого потока", п.3 "Дискреционное управление доступом", п.4.10 "Сетевое взаимодействие"

		сегментами информационной системы, а также между информационными системами				сетевых пакетов, а также атрибутами передаваемой информации (классификационными метками - доступно только для уровня защищенности Максимальный ("Смоленск")).		
4.	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	ОРД + Средства Astra Linux	Разделение полномочий (ролей) пользователей осуществляется администратором с помощью инструментов управления политикой безопасности локально или централизованно в соответствии с организационно-распорядительной документацией оператора.	Управление полномочиями (привилегиями) локальных пользователей (fly-admin-smc), управление полномочиями (привилегиями/ролями) доменных пользователей (ALD/ FreeIPA), дискреционное управление доступом, управление ролями СУБД Дополнительно: Мандатное управление доступом, МКЦ.	РА.1: п.3.3 "Управление пользователями", п.11.6 "Рабочий стол Fly" РКСЗ.1: п.3 "Дискреционное управление доступом", п.4 "Мандатное управление доступом и мандатный контроль целостности" Описание СУБД: п.10 Роли и привилегии в СУБД https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
5.	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	Средства Astra Linux + ОРД	Назначение минимально необходимых прав и привилегий, разделение полномочий (ролей) пользователей осуществляется администратором с помощью инструментов управления политикой безопасности локально или централизованно в соответствии с организационно-распорядительной документацией оператора.	Управление полномочиями (привилегиями) локальных пользователей (fly-admin-smc), управление полномочиями (привилегиями/ролями) доменных пользователей (ALD/ FreeIPA), дискреционное управление доступом, управление ролями СУБД Дополнительно: Мандатное управление	РА.1: п.3.3 "Управление пользователями", п.11.6 "Рабочий стол Fly" РКСЗ.1: п.3 "Дискреционное управление доступом", п.4 "Мандатное управление доступом и мандатный контроль целостности" Описание СУБД: п.10 Роли и привилегии в СУБД

							доступом, МКЦ.	https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
6.	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	Средства Astra Linux + ОРД	Ограничение количества неуспешных попыток входа и блокирования учетной записи и сеанса доступа пользователя при превышении числа неуспешных попыток аутентификации устанавливается администратором с помощью инструментов управления политикой безопасности локально или централизованно.	Управление политикой безопасности локальных пользователей (fly-admin-smc), Управление политикой безопасности доменных пользователей (FreeIPA, ALD)	РА.1: п.3.3 "Управление пользователями" РКС3.1: п.2 "Идентификация и аутентификация" https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
7.	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	-	-	Сторонними программными средствами	-	-	-
8.	УПД.8	Оповещение пользователя			Средства Astra Linux	Сведения о предыдущей аутентификации, количестве	Средства управление рабочим столом Fly (fly-	РА.1: п.11.6 "Рабочий стол Fly"

		после успешного входа в информационную систему о его предыдущем входе в информационную систему				успешных и неуспешных попыток входа предоставляются пользователю автоматически при входе пользователя в систему.	notify-prevlogin)	см. Вывод уведомления о предыдущем входе в систему https://wiki.astralinux.ru/x/eoxsAw (fly-notify-prevlogin)
9.	УПД. 9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы			Средства Astra Linux + ОРД	Ограничение числа параллельных сеансов для каждого пользователя (или группы) осуществляется администратором с помощью инструментов управления политикой безопасности и встроенных программных решений организации распределенного мониторинга.	Системные ограничения ulimits (fly-admin-smc), средства аудита (auditd, zabbix)	РКСЗ.1: п.16.4.3. "Установка квот на использование системных ресурсов" РА.1: п.15 "Средства централизованного протоколирования и аудита" Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc, по работе с программой просмотра файлов журналов ksystemlog
10	УПД. 10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	+	+ 1а, 2	Средства Astra Linux + ОРД	Блокирование сеанса доступа пользователя по истечении заданного администратором времени бездействия осуществляется автоматически или по запросу.	Средства управление рабочим столом Fly (fly-admin-theme)	РА.1: п.11.6 "Рабочий стол Fly" РКСЗ.1: п.17.2 "Указания по эксплуатации ОС" Справка Astra Linux по утилите настройки элементов рабочего стола fly-admin-theme
11	УПД. 11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	+	+	Средства Astra Linux + ОРД, СДЗ	По умолчанию пользователям запрещены любые действия до прохождения процедур идентификации и аутентификации. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Grub (fly-admin-grub2), ограничивающие функции безопасности (astra-nobootmenu-control, astra-autologin-control, astra-hardened-control), защищённая графическая	ОП: п.4.1.2 "Идентификация и аутентификация" РП:1: п.2.1 "Графический вход в систему" РКСЗ.1: п.4.16

						осуществляется администратором путем настройки графического входа в систему и параметров системного загрузчика Grub.	подсистема (fly-admin-dm, fly-dm, fly-qdm)	"Настройка загрузчика GRUB 2" п.16.4.10 "Управление автоматическим входом", п.16.4.12 "Управление загрузкой ядра hardened" п.16.4.18 "Отключение отображения меню загрузчика" Справка Astra Linux по утилитам настройки графического входа в систему fly-admin-dm, запуска серверной части системы fly-dm и поддержки графического интерфейса fly-qdm, настройки загрузчика ОС GRUB2 fly-admin-grub2 https://wiki.astralinux.ru/x/woChAQ (Режим восстановления)
12	УПД. 12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки			Средства Astra Linux + ОРД	В Astra Linux реализовано мандатное управление доступом к информации в процессе ее хранения и обработки с учетом атрибутов безопасности (классификационных меток в формате, установленном ГОСТ Р 58256).	Мандатное управление доступом	РКСЗ.1: п.4.2 "Мандатное управление доступом"
13	УПД. 13	Реализация защищенного удаленного	+ 2, 3	+ 2, 3, 5	VPN-решения/ Средства Astra Linux	Защищенный удаленный доступ через внешние информационно-телекоммуникационные сети	OpenVPN, СКЗИ (VPN-решения)	РА.1: п.6.10 "Средство создания защищенных каналов"

		доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети			+ ОРД	реализуется сертифицированными средствами защиты, предназначенными для построения виртуальных частных сетей (VPN) или средствами Astra Linux, обеспечивающими создание защищенных каналов типа точка-точка или сервер-клиент с использованием свободной реализации технологии виртуальной частной сети.		https://wiki.astralinux.ru/x/PIOhAQ (OpenVPN) https://wiki.astralinux.ru/x/XIV0Ag (СКЗИ)
14	УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+ 1	+ 1, 3	Организационно-технические мероприятия + ОРД + Средства Astra Linux	Реализуется средствами Astra Linux, обеспечивающими контроль использования технологий беспроводного доступа на основе установленной администратором политики выполнения привилегированных действий, дискреционного разграничения доступа и управления устройствами.	Санкции PolicyKit-1, дискреционное управление доступом, управление драйверами/устройствами	РКСЗ.1: п.3 "Дискреционное управление доступом" https://wiki.astralinux.ru/x/Rg1RBg (Блокировка устройств) Справка Astra Linux по работе с утилитами управления политикой безопасности fly-admin-smc, программой управления санкциями PolicyKit-1
15	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+ 1, 2	Организационно-технические мероприятия + ОРД + Средства Astra Linux	Реализуется средствами Astra Linux, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации на основе установленных администратором правил разграничения доступа.	Средства разграничения доступа к подключаемым устройствам (udev)	РА.1: п.17 "Средства разграничения доступа к подключаемым устройствам" РКСЗ.1: п.13 "Контроль подключения съемных машинных носителей информации" https://wiki.astralinux.ru/x/HAKtAg (Съемные носители в Astra Linux) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
16	УПД.16	Управление взаимодействием	+ 1а,	+ 1а,	Организационно-технические	-	-	-

		с информационными системами сторонних организаций (внешние информационные системы)	1б	1б	мероприятия			
17	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники		+ 1	СДЗ, дополнительно: Средства Astra Linux	Доверенная загрузка средств вычислительной техники обеспечивается с использованием средств доверенной загрузки и вспомогательными настройками Astra Linux.	Grub (fly-admin-grub2), ограничивающие функции безопасности (astra-nobootmenu-control, astra-autologin-control, astra-hardened-control)	РКСЗ.1:п.16.4 "Функции безопасности системы"
III. Ограничение программной среды (ОПС)								
1.	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения			Средства Astra Linux + ОРД, СДЗ	Управление запуском (обращениями) в информационной системе разрешенных компонентов программного обеспечения реализуется средствами ограничения программной среды (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")), системным и графическим киоском, а также средствами системных блокировок, настройкой конфигурации загрузчика grub, удалением модулей ядра или запретом их загрузки, управление запуском сервисов, системных служб, приложениями, планированием запуска задач.	ЗПС режим системного киоска, режим киоск Fly, ограничивающие функции безопасности (astra-interpreters-lock, astra-bash-lock, astra-macros-lock, astra-sysrq-lock, astra-ptrace-lock, astra-lkrg-control, astra-modban-lock, astra-noautonet-control, astra-nobootmenu-control, astra-commands-lock, astra-nochmodx-lock, astra-noautonet-control), grub (fly-admin-grub2) управление модулями и параметрами ядра, управление запуском сервисов (fly-admin-service), системных служб (systemgenie), приложениями (fly-admin-autostart), планированием запуска задач (fly-admin-cron)	РКСЗ.1:п.16.1 "Замкнутая программная среда", п.16.2 "Режим Киоск-2", п.16.4 "Функции безопасности системы" https://wiki.astralinux.ru/x/6oR0Ag (Режим замкнутой программной среды) https://wiki.astralinux.ru/x/wYZ-Bg (Инструменты командной строки astra-safepolicy) Справка Astra Linux по утилитам настройки загрузчика ОС GRUB2 fly-admin-grub2, запуска сервисов fly-admin-sevice, системных служб systemgenie, приложений fly-admin-autostart, планирования запуска задач fly-admin-cron

2.	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		+	Средства Astra Linux + ОРД	Задача установки в информационную систему разрешенного программного обеспечения реализуется администратором с использованием средств управления программными пакетами и средств контроля целостности. Контроль установки в информационную систему разрешенного программного обеспечения может быть реализован с использованием средств регламентного контроля целостности устанавливаемого программного обеспечения и средств динамического контроля целостности в составе доверенного служебного репозитория с использованием хэш-функции или электронной цифровой подписи (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")). Применение и контроль параметров настройки компонентов программного обеспечения могут быть реализованы с использованием программных средств управления конфигурациями.	Управление программными пакетами (synaptik), редактор репозиториев (fly-admin-repo), проверка целостности системы (fly-admin-int-check), контроль целостности пакетов ПО (gostsum), средства управления конфигурациями (Ansible/Puppet/Foreman) Дополнительно: ЗПС	РА.1: п.5 "Управление программными пакетами", п.6.11 "Средство удаленного администрирования Ansible" ОП: п.4.1.9 "Контроль целостности" РКСЗ.1: п.16 "Ограничение программной среды", п.9 "Контроль целостности" https://wiki.astralinux.ru/x/QQLGBw (Инструмент «Редактор репозиториев») https://wiki.astralinux.ru/x/OwAy (Подключение репозиториев) https://wiki.astralinux.ru/x/6oR0Ag (Режим замкнутой программной среды) https://wiki.astralinux.ru/x/UAHUCg (Подсчет контрольных сумм в deb-пакетах) Справка Astra Linux по утилитам Редактор репозиториев fly-admin-repo, Проверка целостности fly-admin-int-check
3.	ОПС. 3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его	+	+	Средства Astra Linux + ОРД, Орг.мерами (обеспечивающими контроль выполнения условий и сроков действия	Задача установки в информационную систему разрешенного программного обеспечения реализуется администратором в соответствии с ОРД с использованием средств управления программными пакетами, средств регламентного контроля целостности устанавливаемого	Управление программными пакетами (synaptik), проверка целостности системы (fly-admin-int-check) Дополнительно: ЗПС	РА.1: п.5 "Управление программными пакетами" ОП: п.4.1.9 "Контроль целостности" РКСЗ.1: п.16 "Ограничение

		компонентов			сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков)	программного обеспечения и средств динамического контроля целостности в составе доверенного служебного репозитория с использованием хэш-функции или электронной цифровой подписи (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")). Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов осуществляется только от имени администратора (PolicyKit) в соответствии с УПД.5.		программной среды", п.9 "Контроль целостности" https://wiki.astralinux.ru/x/OwAy (Подключение репозиториев) https://wiki.astralinux.ru/x/QQLGBw (Инструмент «Редактор репозиториев» fly-admin-repo) Справка Astra Linux по утилитам Редактор репозиториев fly-admin-repo, Проверка целостности fly-admin-int-check
4.	ОПС. 4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов			Средства Astra Linux + ОРД	Исключение возможности хранения временных файлов и несанкционированных действий с ними, а также доступа пользователя к «остаточной» информации реализуется с использованием механизмов очистки оперативной и внешней памяти (доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")) и встроенного в ядро Astra Linux механизма изоляции процессов.	Ядро - механизм очистки памяти (astra-secdel-control), механизм очистки разделов подкачки (astra-swapwiper-control), изоляция процессов	РКСЗ.1: п.7 "Изоляция процессов", п.8 "Защита памяти", п.16.4.29 "Управление безопасным удалением файлов", п.16.4.30. "Управление очисткой разделов подкачки"
IV. Защита машинных носителей информации (ЗНИ)								
1.	ЗНИ. 1	Учет машинных носителей информации	+	+ 1а	Организационные мероприятия, ОРД	-	-	-
2.	ЗНИ. 2	Управление доступом к машинным носителям информации	+	+	Организационные мероприятия, ОРД	-	-	-

3.	ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны			Организационные мероприятия, ОРД	-	-	-
4.	ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах			Организационно-технические мероприятия	-	-	-
5.	ЗНИ.5	Контроль использования интерфейсов ввода (вывода)		+	Организационно-технические мероприятия, ОРД, Средства Astra Linux	Реализуется средствами Astra Linux, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых вешних программно-аппаратных устройств и конкретных съемных машинных носителей информации на основе установленных администратором правил разграничения доступа.	Средства разграничения доступа к подключаемым устройствам (udev), управление драйверами	РКСЗ.1: п.13 "Контроль подключения съемных машинных носителей информации" https://wiki.astralinux.ru/x/HAKtAg (Съемные носители в Astra Linux)

6.	ЗНИ.6	Контроль подключения машинных носителей информации			Средства Astra Linux + ОРД	Реализуется средствами Astra Linux, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации на основе установленных администратором правил разграничения доступа.	Средства разграничения доступа к подключаемым устройствам (udev, astra-mount-lock)	РКСЗ.1: п.13 "Контроль подключения съемных машинных носителей информации", п.6 "Регистрация событий безопасности", п.14 "Сопоставление пользователя с устройством" https://wiki.astralinux.ru/x/HAKtAg (Съемные носители в Astra Linux)
7.	ЗНИ.7	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	+ 1,5б	+ 1, 5в	Организационно-технические мероприятия, Средства Astra Linux + ОРД, Усиление 5в, 5г: сторонние средства гарантированного уничтожения информации	Задача уничтожения (стирания) информации, исключения возможности восстановления защищаемой информации реализуется с помощью средств защиты памяти, настройки параметров использования машинных носителей, средств затирания данных.	Средства затирания данных (dd, shred) Дополнительно: Механизм очистки памяти (astra-secdel-control)	РКСЗ.1: п.13 "Контроль подключения съемных машинных носителей информации", п.16.4.20 "Запрет монтирования съемных носителей", п.6 "Регистрация событий безопасности" https://wiki.astralinux.ru/x/HAKtAg (Съемные носители в Astra Linux)
8.	ЗНИ.8	Контроль ввода (вывода) информации на машинные носители информации			Средства Astra Linux + ОРД	Реализуется средствами Astra Linux, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации на основе установленных администратором правил разграничения доступа.	Средства разграничения доступа к подключаемым устройствам (udev)	РКСЗ.1: п.8 "Защита памяти" Справка Astra Linux по работе с утилитой форматирования внешних носителей fly-admin-format
V. Регистрация событий безопасности (РСБ)								
1.	РСБ.1	Определение событий	+	+ 1,3,	ОРД	События безопасности, подлежащие регистрации, и сроки их хранения	-	-

		безопасности, подлежащих регистрации, и сроков их хранения		4а		определяются администратором.		
2.	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+ 1а	ОРД	Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются администратором.	-	-
3.	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	+	+ 1	Средства Astra Linux + ОРД, SIEM	Сбор, запись и хранение информации о событиях безопасности осуществляются с помощью средств централизованного протоколирования и ведения журналов аудита событий безопасности, установленных администратором, хранения записей системных журналов и записей о событиях безопасности в обособленном хранилище. Для своевременного выявления инцидентов и реагирования на них в информационной системе используются системы управления событиями безопасности (SIEM).	Средства аудита (auditd, zabbix), Системный журнал (ksystemlog,system-config-audit)	РА.1: п.15 "Средства централизованного протоколирования и аудита" РКСЗ.1: п.6 "Регистрация событий безопасности" https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix) Справка Astra Linux по работе с утилитой управления политикой безопасности fly-admin-smc и утилитой конфигурации аудита system-config-audit, по работе с программой просмотра файлов журналов ksystemlog
4.	РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе	+	+	Средства Astra Linux + ОРД	Реагирование на сбои регистрации и предупреждения администратора при заполнении объема памяти для хранения информации о событиях безопасности осуществляются с помощью средств централизованного	Средства аудита (zabbix)	РА.1: п.15 "Средства централизованного протоколирования и аудита" https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для

		аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				протоколирования и аудита событий безопасности.		Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix)
5.	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	+	Средства Astra Linux + ОРД, Организационные мероприятия, SIEM, СОВ	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности реализуется с использованием средств организации распределенного мониторинга сети и жизнеспособности и целостности серверов. С целью выявления инцидентов безопасности и реагирования на них в информационной системе могут использоваться сертифицированные системы управления событиями безопасности (SIEM) и системы обнаружения вторжений.	Средства аудита (auditd, zabbix), Системный журнал (ksystemlog)	РА.1: п.15 "Средства централизованного протоколирования и аудита" https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix) Справка по работе с программой просмотра файлов журналов ksystemlog
6.	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+	+	Средства Astra Linux	Синхронизация системного времени в информационной системе реализуется с использованием встроенных в Astra Linux служб синхронизации времени.	Службы синхронизации времени (ntpd, chronyd, timesyncd, linuxptp)	РА.1: п.6.7 (Службы точного времени) https://wiki.astralinux.ru/x/l4GhAQ (Службы синхронизации времени)
7.	РСБ.7	Защита информации о событиях безопасности	+	+ 1	Средства Astra Linux + ОРД	Защита информации о событиях безопасности реализуется монитором обращений в соответствии с реализованными правилами разграничения доступа к журналам аудита.	Средства аудита (auditd, zabbix), Дискреционное управление доступом Дополнительно: Мандатное управление доступом	РА.1: п.15 "Средства централизованного протоколирования и аудита" РКС3.1: п.3 "Дискреционное управление доступом", п.4.2 "Мандатное управление доступом"

								https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix) Справка Astra Linux по работе с программой просмотра файлов журналов ksystemlog
8.	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе			Средства Astra Linux + ОРД	Возможность осуществления просмотра и анализа информации о действиях пользователей предоставляется администратору (пользователям в соответствии с установленными правилами разграничения доступа) с использованием средств централизованного протоколирования и ведения журналов аудита событий безопасности	Средства аудита (auditd, zabbix)	РА.1: п.15 "Средства централизованного протоколирования и аудита" https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix) Справка Astra Linux по работе с программой просмотра файлов журналов ksystemlog
VI. Антивирусная защита (АВЗ)								
1.	АВЗ.1	Реализация антивирусной защиты	+ 1	+ 1, 2	-	-	-	-
2.	АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+ 1	-	-	-	-
VII. Обнаружение вторжений (СОВ)								
1.	СОВ.1	Обнаружение вторжений		+ 2	-	-	-	-
2.	СОВ.2	Обновление базы решающих правил		+	-	-	-	-
VIII. Контроль (анализ) защищенности информации (АНЗ)								

1.	АН3. 1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+ 1,4	+ 1, 2,4	Средства анализа (контроля) защищенности (сканеры безопасности), ОРД, Организационные мероприятия, Средства Astra Linux	Выявление и оперативное устранение уязвимостей Astra Linux производится разработчиком в соответствии с «Требованиями к уровням доверия», утвержденным приказом ФСТЭК России №76, и ГОСТ Р 56939.	Обновление ОС, fly-astra-update, fly-update-notifier	ОП: п.3 "Порядок обновления ОС" Справка по работе с утилитой установки обновлений с возможностью гибкой настройки fly-astra-update, с утилитой "Проверка обновлений" fly-update-notifier https://wiki.astralinux.ru/x/2xZIB (fly-astra-update)
2.	АН3. 2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	Средства Astra Linux + ОРД	Обновление безопасности производится администратором согласно документации на Astra Linux. Контроль целостности обновлений Astra Linux может быть реализован с использованием регламентного контроля целостности с использованием функции хэширования и сверки полученного значения с эталонным, указанным в специальном файле с контрольными суммами, входящем в состав обновлений безопасности, а также организацией доверенного служебного репозитория с использованием хэш-функции или электронной цифровой подписи для режима ЗПС (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")). Контроль установки обновлений Astra Linux выполняется одним из следующих способов: - в «ручном» режиме путём сравнивания списка установленных обновлений со списком обновлений, зафиксированным в журнале	Обновление ОС, контроль целостности сторонних файлов (gostsum) Дополнительно: Ansible, доверенный репозиторий (МКЦ)	ОП: п.3.2 "Внеочередное (оперативное) обновление" РА.1: п.6.11 "Средство удаленного администрирования Ansible" https://wiki.astralinux.ru/x/X4AmAg (Оперативные обновления для Astra Linux) Справка по работе с утилитой установки обновлений с возможностью гибкой настройки fly-astra-update

						установки обновлений; - автоматизированный контроль установленных обновлений с использованием программы "Проверка обновлений"; - автоматизированный контроль установленных обновлений с использованием программных средств (например, Ansible), предусмотренных к использованию условиями эксплуатации обновляемого программного обеспечения или с применением сертифицированных ФСТЭК России средств анализа защищенности (сканеров безопасности).		
3.	АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	+	+ 1	Средства Astra Linux + ОРД	Контроль работоспособности встроенного комплекса средств защиты информации Astra Linux осуществляется с помощью автоматического и регламентного тестирования функций безопасности, контролем соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации, и восстановлением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов в соответствии с ОЦЛ.3	Тестирование СЗИ Средства резервного копирования (Bacula, dd, tar, luckybackup, rsync), Средства восстановления повреждённых и удалённых данных (ddrescue, testdisk), режим восстановления ОС, механизм проверки и восстановления ФС (fsck), Восстановление СУБД (SQL-дамп, резервное копирование, непрерывное архивирование) средства управления конфигурациями (Ansible/Puppet/Foreman)	РКС3.2 РА.1: п.16 "Резервное копирование и восстановление данных", п.6.11 "Средство удаленного администрирования Ansible" РКС3.1: п.10 "Надежное функционирование" https://wiki.astralinux.ru/x/woChAQ (Режим восстановления) https://wiki.astralinux.ru/x/roh0Ag (Архивирование и восстановление файлов с сохранением мандатных атрибутов) https://wiki.astralinux.ru/x/dQHGAg (BACULA) https://wiki.astralinux.ru/x/iYPGBg (Средства восстановления повреждённых и удалённых данных)

4.	АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+ 1	Средствами Astra Linux, ОРД, Орг.мерами (визуальной проверкой может обеспечиваться контроль состава технических средств и средств защиты информации, требуемые, соблюдение правил эксплуатации и неизменности конфигурации ИС в ходе эксплуатации, контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации)	Контроль программного обеспечения и средств защиты информации осуществляется в соответствии с ОПС.1-3, регистрация событий и удаления программ - в соответствии с РСБ.3. Контроль установленного в Astra Linux оборудования можно осуществлять с использованием специализированных утилит.	Контроль целостности (afick, fly-admin-int-check), средства аудита (auditd, zabbix), средства контроля установленного оборудования (lspci, lshw, lsusb).	ОП: п.4.1.9 "Контроль целостности" РА.1: п.15 "Средства централизованного протоколирования и аудита", РКС3.1: п.9 "Контроль целостности" https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix) https://wiki.astralinux.ru/x/k4-NAw (определение оборудования) Справка по работе с утилитой проверки целостности fly-admin-int-check
5.	АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	+	+ 1	Средства Astra Linux + ОРД, Организационные мероприятия	Контроль осуществляется путем анализа содержимого журналов регистрации событий безопасности для мер защиты УПД.1-УПД.6	Средства аудита (auditd, zabbix)	РА.1: п.15 "Средства централизованного протоколирования и аудита" https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc

IX. Обеспечение целостности информационной системы и информации (ОЦЛ)								
1.	ОЦЛ. 1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации		+ 1, 3	Средствами Astra Linux, Организационные мероприятия (в конфиденциальном сегменте информационной системы обеспечивается физическая защита технических средств информационной системы в соответствии с идентификаторами мер «ЗТС.2» и «ЗТС.3»), ОРД.	Для обеспечения контроля целостности программного обеспечения и средств защиты информации используются средства динамического (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")) и регламентного контроля целостности, автоматического и регламентного тестирования функций безопасности.	Контроль целостности (afick, fly-admin-int-check), контроль целостности пакетов ПО (gostsum), Тестирование СЗИ Дополнительно: ЗПС	РКСЗ.1: п.9 "Контроль целостности" РКСЗ.2 https://wiki.astralinux.ru/x/UAHUCg (Подсчет контрольных сумм в deb-пакетах) Справка по работе с утилитой проверки целостности fly-admin-int-check
2.	ОЦЛ. 2	Контроль целостности информации, содержащейся в базах данных информационной системы			Средствами Astra Linux, ОРД, Организационные мероприятия (в конфиденциальном сегменте информационной системы обеспечивается физическая защита технических средств информационной системы в соответствии с идентификаторами мер «ЗТС.2» и «ЗТС.3»)	Контроль целостности информации реализуется с использованием средств регламентного контроля целостности.	Контроль целостности (afick)	ОП: п.4.1.9 "Контроль целостности" РКСЗ.1: п.9 "Контроль целостности"
3.	ОЦЛ. 3	Обеспечение возможности восстановления программного	+	+	Средства Astra Linux, ОРД	В целях обеспечения возможности восстановления работоспособности системы используется режим восстановления и средства	Средства резервного копирования (Bacula, dd, tar, luckybackup, rsync), Средства восстановления	РА.1: п.16 "Резервное копирование и восстановление данных" РКСЗ.1: п.10 "Надежное

		обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				резервного копирования.	повреждённых и удалённых данных (ddrescue, testdisk), механизм проверки и восстановления ФС (fsck), режим восстановления ОС Восстановление СУБД (SQL-дамп, резервное копирование, непрерывное архивирование)	функционирование" https://wiki.astralinux.ru/x/woChAQ (Режим восстановления) https://wiki.astralinux.ru/x/roh0Ag (Архивирование и восстановление файлов с сохранением мандатных атрибутов) https://wiki.astralinux.ru/x/dQHGAg (BACULA) https://wiki.astralinux.ru/x/iYPGBg (Средства восстановления повреждённых и удалённых данных)
4.	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)		+	Сторонние ПС			-
5.	ОЦЛ. 5	Контроль содержания информации, передаваемой из информационной системы (контейнерный,			Средствами Astra Linux, Организационные мероприятия, ОРД	Контроль содержания информации, основанный на свойствах объектов доступа, осуществляется согласно установленной политики дискреционного и мандатного управления доступом (мандатное управление доступом доступно	Мандатное управление доступом, Дискреционное управление доступом, контроль подключения съемных машинных носителей информации, Защищенный комплекс	РКСЗ.1: п.3 "Дискреционное управление доступом", п.4.2 "Мандатное управление доступом", п.13 "Контроль подключения съемных

		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				только для уровня защищенности Astra Linux "Максимальный" ("Смоленск")).	программ печати и маркировки документов (cups)	машинных носителей информации", п.14 "Сопоставление пользователя с устройством" РА.1: п.12 "Защищенный комплекс программ печати и маркировки документов"
6.	ОЦЛ. 6	Ограничение прав пользователей по вводу информации в информационную систему			Средствами Astra Linux, ОРД, Организационные мероприятия, возможна реализация на уровне прикладного ПО.	Ввод пользователями информации осуществляется строго с учетом и в соответствии с установленными правилами разграничения доступа (УПД.2, УПД.4) на основе типа операции (чтение, запись, исполнение), контекста безопасности пользователя и классификационной метки объекта (мандатное управление доступом доступно только для уровня защищенности Astra Linux "Максимальный" ("Смоленск")).	Мандатное управление доступом, Дискреционное управление доступом, режим системного киоска, режим киоск Fly, МКЦ	РКСЗ.1: п.3 "Дискреционное управление доступом", п.4 "Мандатное управление доступом и мандатный контроль целостности", п.16.2 "Режим Киоск-2"
7.	ОЦЛ. 7	Контроль точности, полноты и правильности данных, вводимых в информационную систему			Прикладное ПО, Средства Astra Linux (СУБД)	Контроль точности, полноты и правильности данных, вводимых в информационную систему путем установления и проверки соблюдения форматов ввода данных, синтаксических, семантических и (или) иных правил ввода информации в информационную систему (допустимые наборы символов, размерность, область числовых	СУБД	РА.2

						значений, допустимые значения, количество символов) для подтверждения того, что ввод информации соответствует заданному оператором формату и содержанию осуществляется с использованием прикладного ПО и средств СУБД.		
8.	ОЦЛ. 8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			Прикладное ПО, Средства Astra Linux	Контроль осуществляется средствами протоколирования и аудита событий (в том числе, действий пользователя) в соответствии с установленными правилами разграничения доступа.	Средства аудита (auditd, zabbix) Дискреционное управление доступом Дополнительно: Мандатное управление доступом, МКЦ, СУБД	РКС3.1: п.3 "Дискреционное управление доступом", п.4 "Мандатное управление доступом и мандатный контроль целостности" РА.1: п.15 "Средства централизованного протоколирования и аудита" https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix)
X. Обеспечение доступности информации (ОДТ)								
1.	ОДТ. 1	Использование отказоустойчивых технических средств			Организационно-технические мероприятия, ОРД Дополнительно: Средства Astra Linux	Возможность работы Astra Linux на нескольких технических средствах в отказоустойчивом режиме обеспечивает доступность сервисов и информации при выходе из строя одного из технических средств (отказоустойчивый кластер). Контроль с установленной оператором периодичностью за значениями характеристик (коэффициентов) готовности и надежности технических средств осуществляется с использованием средств централизованного протоколирования и аудита.	Системные ограничения ulimits (fly-admin-smc), средства аудита (zabbix) Дополнительно: Средства обеспечения отказоустойчивости и высокой доступности (Pacemaker и Corosync, Keepalived, Ceph, HAProxy, bounding), программный RAID, резервирование в домене (FreeIPA, ALD), репликация в домене (FreeIPA)	РКС3.1: п.16.4.3 "Установка квот на использование системных ресурсов" РА.1: п.7 "Средства обеспечения отказоустойчивости и высокой доступности", п.3.1.5 "Программная организация разделов RAID и тома LVM", п.8.3.8.2 "Создание резервного сервера FreeIPA", п.8.2.6.9 "Создание резервного сервера ALD", п.15 "Средства

								централизованного протоколирования и аудита" Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc
2.	ОДТ. 2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы			Организационно-технические мероприятия, ОРД, Средства Astra Linux	Средства организации ЕПП Astra Linux предоставляют возможность развертывания основного и резервных контроллеров домена, обеспечивающих ведение двух или более программных средств СЗИ НСД и баз данных безопасности. В Astra Linux существует возможность в процессе загрузки после сбоя автоматически выполнять программу проверки и восстановления ФС - fsck. Если сбой привел к выводу из строя жестких дисков, следует заменить вышедшее из строя оборудования и переустановить Astra Linux с диска с дистрибутивом, а пользовательские данные восстановить с резервной копии. Резервное копирование используется для восстановления файлов, случайно удаленных пользователями или утерянных из-за отказов устройств хранения, получения периодически создаваемых снимков состояния данных, получения данных для восстановления после аварий. В состав Astra Linux входят средства комплекс программ Bacula, утилиты rsync и tar для выполнения операций резервного копирования и восстановления объектов ФС с сохранением и восстановлением мандатных атрибутов и атрибутов	Средства обеспечения отказоустойчивости и высокой доступности (Pacemaker и Corosync, Keepalived, Ceph, HAProxy, bounding), программный RAID, резервирование в домене (FreeIPA, ALD), репликация в домене (FreeIPA), средства резервного копирования (Bacula, dd, tar, luckybackup, rsync), Восстановление СУБД (SQL-дамп, резервное копирование, непрерывное архивирование), Средства восстановления повреждённых и удалённых данных (ddrescue, testdisk), механизм проверки и восстановления ФС (fsck)	РА.1: п.7 "Средства обеспечения отказоустойчивости и высокой доступности", п.3.1.5 "Программная организация разделов RAID и тома LVM", п.8.3.8.1 "Создание резервной копии и восстановление", п.8.3.8.2 "Создание резервного сервера FreeIPA", п.8.2.6.9 "Создание резервного сервера ALD", п.16 "Резервное копирование и восстановление данных" РКС3.1 п.10 "Надежное функционирование" https://wiki.astralinux.ru/x/niaaBg (Агрегация каналов (bonding))

						аудита. Возможность работы Astra Linux на нескольких технических средствах в отказоустойчивом режиме обеспечивает доступность сервисов и информации при выходе из строя одного из технических средств (отказоустойчивый кластер). Резервирование каналов связи осуществляется с использованием специальных утилит, позволяющих производить агрегацию каналов связи.		
3.	ОДТ. 3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование		+	Организационные мероприятия, ОРД, Средства Astra Linux	Контроль за состоянием информационной системы осуществляется путем регистрации событий и анализа содержимого системных журналов, и принятия мер по восстановлению отказавших средств в соответствии с ОЦЛ.3.	Средства аудита (auditd, zabbix), системные ограничения ulimits (fly-admin-smc)	РА.1: п.15 "Средства централизованного протоколирования и аудита" РКС3.1: п.16.4.3 "Установка квот на использование системных ресурсов" https://wiki.astralinux.ru/x/E4NOAg (Шаблоны для Zabbix) https://wiki.astralinux.ru/x/-4JOAg (Zabbix) Справка Astra Linux по работе с программой просмотра файлов журналов ksystemlog
4.	ОДТ. 4	Периодическое резервное копирование информации на резервные машинные носители информации		+ 1, 2	Организационные мероприятия, Средства Astra Linux, ОРД	Резервное копирование осуществляется с использованием специальных программ и утилит, позволяющих восстанавливать информацию и объекты файловой системы с сохранением их атрибутов безопасности и аудита.	Средства резервного копирования (Bacula, dd, tar, luckybackup, rsync), Резервирование в домене (ALD, FreeIPA), Восстановление СУБД (SQL-дамп, резервное копирование, непрерывное архивирование), Средства восстановления повреждённых и удалённых	РА.1: п.16 "Резервное копирование и восстановление данных", п.8.3.8.1 "Создание резервной копии и восстановление", п.8.2.6.9 "Создание резервного сервера ALD" РКС3.1 п.10 "Надежное

							данных (ddrescue, testdisk), механизм проверки и восстановления ФС (fsck)	функционирование" https://wiki.astralinux.ru/x/dQHGAg (BACULA) https://wiki.astralinux.ru/x/roh0Ag (Архивирование и восстановление файлов с сохранением мандатных атрибутов)
5.	ОДТ. 5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала		+	Организационно-технические мероприятия, ОРД, Средства Astra Linux	Резервное копирование осуществляется с использованием программ и утилит, позволяющих восстанавливать информацию и объекты файловой системы, и сервисов планирования выполнения заданий.	Средства резервного копирования (Bacula, dd, tar, luckybackup, rsync), Резервирование в домене (ALD, FreeIPA), планированием запуска задач (fly-admin-cron), Восстановление СУБД (SQL-дамп, резервное копирование, непрерывное архивирование), Средства восстановления повреждённых и удалённых данных (ddrescue, testdisk), механизм проверки и восстановления ФС (fsck)	РА.1: п.16 "Резервное копирование и восстановление данных", п.8.3.8.2 "Создание резервного сервера FreeIPA", п.8.2.6.9 "Создание резервного сервера ALD" РКС3.1 п.10 "Надежное функционирование" https://wiki.astralinux.ru/x/dQHGAg (BACULA) https://wiki.astralinux.ru/x/roh0Ag (Архивирование и восстановление файлов с сохранением мандатных атрибутов) Справка Astra Linux по работе с утилитой планирования запуска задач fly-admin-cron
6.	ОДТ. 6	Кластеризация информационной системы и (или) ее сегментов			Организационно-технические мероприятия, ОРД, Средства Astra Linux	Возможность работы Astra Linux на нескольких технических средствах в отказоустойчивом режиме обеспечивает доступность сервисов и информации при выходе из строя одного из технических средств (отказоустойчивый кластер).	Средства обеспечения отказоустойчивости и высокой доступности (Pacemaker и Corosync, Keepalived, Ceph, HAProxy, bounding), репликация в домене (FreeIPA)	ОП: п.4.1.15 "Обеспечение работы в отказоустойчивом режиме" РА1: п.7 "Средства обеспечения отказоустойчивости и высокой доступности", п.8.3.8.2 "Создание резервного сервера FreeIPA"

								https://wiki.astralinux.ru/x/niaaBg (Агрегация каналов (bonding))
7.	ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей), в том числе по передаче информации		+	Организационные мероприятия, ОРД	-	-	-
XII. Защита технических средств (ЗТС)								
1.	ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам			Организационно-технические мероприятия			-
2.	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционировани	+	+	Организационно-технические мероприятия			-

		я						
3.	ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционировани я, а также в помещения и сооружения, в которых они установлены, исключающие несанкционирова нный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционировани я информационной системы и помещения и сооружения, в которых они установлены	+	+	Организационно-технические мероприятия, СДЗ	-	-	-
4.	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее	-	-	Организационно-технические мероприятия	-	-	-

		несанкционированный просмотр						
5.	ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)			Организационно-технические мероприятия	-	-	-
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)								
1.	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		+ 3	Организационно-технические мероприятия, ОРД, Средства Astra Linux	Разделение функций по управлению (администрированию) системой в целом и системой защиты информации, функций по обработке информации осуществляется согласно ОРД локально или централизованно с использованием средств управления политикой безопасности.	Управление полномочиями (привилегиями) локальных пользователей (fly-admin-smc), управление полномочиями (привилегиями/ролями) доменных пользователей (ALD/ FreeIPA), Санкции PolicyKit-1, дискреционное управление доступом, средства организации домена Дополнительно: Системный и графический киоск	см. раздел II. УПД РА.1: п.3.3 "Управление пользователями", п.4.1.3 "Организация ЕПП" РКСЗ.1: п.3 "Дискреционное управление доступом", п.4 "Мандатное управление доступом и контроль целостности", https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) https://wiki.astralinux.ru/x/zQC4B (Режим киоска) Справка Astra Linux по утилите управления политикой безопасности fly-admin-smc, программой управления санкциями PolicyKit-1
2.	ЗИС.2	Предотвращение задержки или прерывания			Средства Astra Linux	Предотвращение задержки или прерывания выполнения процессов осуществляется с использованием	Системные сервисы и компоненты (nice, renice, kill, nohup, ps)	РА.1: п.4.3.2 "Администрирование многопользовательской

		выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				утилит управления приоритетами процессов.		и многозадачной среды"
3.	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	+	+	Организационно-технические мероприятия (СКЗИ), ОРД, Средства Astra Linux	Обеспечение защиты информации при ее передаче обеспечивается средствами контроля целостности передаваемой информации и использованием защищенных каналов, реализуется сертифицированными средствами защиты, предназначенными для построения виртуальных частных сетей (VPN) или средствами Astra Linux, обеспечивающими создание защищенных каналов типа точка-точка или сервер-клиент с использованием свободной реализации технологии виртуальной частной сети.	OpenVPN, СКЗИ, Средства контроля целостности (сервис электронной подписи)	РА.1: п.6.10 "Средство создания защищенных каналов" РКСЗ.1: п.9.5 «Сервис электронной подписи» https://wiki.astralinux.ru/x/PIOhAQ (OpenVPN) https://wiki.astralinux.ru/x/XIV0Ag (СКЗИ)
4.	ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)			Организационно-технические мероприятия (СКЗИ), Средства Astra Linux	Доверенный канал обеспечивается: - локально функциями аутентификации и сохранением контекста; - в ЛВС при сетевом доступе встроенными в Astra Linux средствами создания защищенных каналов и (или) средствами организации ЕПП; - при межсетевом доступе внешними средствами создания защищенных каналов.	OpenVPN, СКЗИ, Средства организации ЕПП	РА.1: п.6.10 "Средство создания защищенных каналов", п.3 "Системные компоненты", п.4 "Системные сервисы, состояния и команды" РКСЗ.1: п.7.1 "Изоляция процессов"
5.	ЗИС.5	Запрет несанкционирова	+	+ 1	Организационно-технические	Запрет реализуется с помощью исключения или блокирования	Средства межсетевого экранирования	РКСЗ.1: п.11 "Фильтрация сетевого

		нной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств			мероприятия (СКЗИ), Средства Astra Linux	доступа к модулям, отвечающим за работу соответствующих периферийных устройств, в соответствии с установленными правилами разграничения доступа, а также применением механизма фильтрации сетевых пакетов.	(astra-ufw-control), дискреционное управление доступом, управление драйверами/устройствами	потока", п.3 "Дискреционное управление доступом" РА.1: п.3 "Системные компоненты", п.4 "Системные сервисы, состояния и команды" https://wiki.astralinux.ru/x/Rg1RBg (Блокировка устройств) Справка Astra Linux по работе с утилитами управления политикой безопасности fly-admin-smc, программой управления санкциями PolicyKit-1
6.	ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационным и системами			Организационно-технические мероприятия (СКЗИ, МЭ и/или средств однонаправленной передачи информации, поддерживающими форматы атрибутов безопасности), Средства Astra Linux	Защита реализуется с применением сертифицированных средств защиты информации, реализующих функции контроля и фильтрации сетевого потока, поддерживающих управление сетевыми потоками с использованием классификационных меток. Передача и контроль целостности атрибутов информации осуществляется Astra Linux в соответствии с политикой управления доступом с учетом атрибутов передаваемой информации (классификационными метками - доступно только для уровня защищенности Астра Linux "Максимальный" ("Смоленск")). Целостность заголовка IP-пакетов, содержащего классификационную метку, обеспечивается с применением средств защиты канала передачи информации	Мандатное управление доступом (передача и контроль меток конфиденциальности при передаче информации по сети), Средства межсетевого экранирования (astra-ufw-control), СКЗИ (OpenVPN)	РА.1: п.6.10 "Средство создания защищенных каналов" РКСЗ.1: п.4.10 "Сетевое взаимодействие", п.9 "Контроль целостности", п.11 "Фильтрация сетевого потока"
7.	ЗИС.7	Контроль санкционированн		+ 1	Средства Astra Linux + ОРД	В составе установочного диска Astra Linux отсутствуют средства	Средства аудита (auditd, zabbix), ограничивающие	РКСЗ.1: п.6 "Регистрация событий

		ого 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				связанные с технологиями мобильного кода использующими Java, ActiveX, VBScript. Исключение несанкционированного использования технологий (запрета исполнения и несанкционированного использования кода) реализуется средствами создания ограничения программной среды, в частности созданием «замкнутой программной среды» (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")). Контроль осуществляется с помощью инструментов регистрации и анализа событий безопасности в системных журналах.	функции безопасности (astra-interpreters-lock), ЗПС	безопасности", п.16 "Ограничение программной среды", п.16.4 "Функции безопасности системы" РА.1: п.15 "Средства централизованного протоколирования и аудита" https://wiki.astralinux.ru/x/6oR0Ag (Режим замкнутой программной среды)
8.	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		+	Организационно-технические мероприятия, ОРД			-

		передачи речи						
9.	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		+	Организационно-технические мероприятия, ОРД			-
10	ЗИС. 10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам			Средства Astra Linux	Подтверждение происхождения источника получаемой информации осуществляется службой DNS (системой доменных имен).	DNS	РА.1: п.6.5 "Служба DNS" https://wiki.astralinux.ru/x/yIOhAQ (DNS-сервер BIND9)
11	ЗИС. 11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых		+	Организационно-технические мероприятия (СКЗИ, МЭ), Средства Astra Linux	Подлинность сетевых соединений обеспечивается средствами организации сквозной доверенной аутентификации, использованием защищенных каналов и проверкой целостности передаваемых пакетов совместно со средствами Astra Linux, реализующими функции контроля и фильтрации проходящих	OpenVPN, СКЗИ, Средства межсетевого экранирования (astra-ufw-control), Организация ЕПП (Kerberos)	РКСЗ.1: п.11 "Фильтрация сетевого потока" РА.1: п.6.10 "Средство создания защищенных каналов", п.8.1 "Архитектура ЕПП"

		устройств и сервисов				информационных потоков в соответствии с заданными правилами.		
12	ЗИС. 12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю		+	-	-	-	-
13	ЗИС. 13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя		+	-	-	-	-
14	ЗИС. 14	Использование устройств терминального доступа для обработки информации			Организационно-технические мероприятия, СКЗИ, Средства Astra Linux	Возможность обработки информации с помощью устройств терминального доступа реализуется средствами реализации терминального сервера, технологией «тонкого клиента» в сетях с клиент-серверной или терминальной архитектурой и службой виртуальных рабочих столов.	LTSP	https://wiki.astralinux.ru/x/EIQyAw
15	ЗИС. 15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки		+	Средства Astra Linux	Защита файлов, не подлежащих изменению, реализуется средствами контроля целостности объектов файловой системы, средствами ограничения программной среды (режим ЗПС -доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")), установкой правил разграничения доступа.	Контроль целостности (Afick), Дополнительно: Контроль расширенных атрибутов (ЗПС), МКЦ	РКСЗ.1: п.3 "Дискреционное управление доступом", п.4.3 "Мандатный контроль целостности", п.9.4 "Средства регламентного контроля целостности", п.16 "Ограничение программной среды"

		информации						
16	ЗИС. 16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов			Средства Astra Linux	В Astra Linux идентифицированы и приведены условия исключения скрытых каналов передачи информации в соответствии с «Требованиями к уровням доверия», утвержденным приказом ФСТЭК России №76. Условиями исключения скрытых каналов является реализуемая Astra Linux политика дискреционного и мандатного управления доступом (мандатное управление доступом доступно только для уровня защищенности Astra Linux "Максимальный" ("Смоленск")), мандатного контроля целостности, а также возможность изоляции процессов в совокупности с очисткой областей оперативной памяти и обеспечение запуска процессов в замкнутой относительно остальных процессов среде по памяти (режимы МКЦ и механизм очистки освобождаемой внешней памяти доступны для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")).	Мандатное управление доступом, МКЦ, Дискреционное управление доступом, Изоляция процессов, Очистка памяти (secdel), режим киоска, блокировка запуска программ df,chattr,arp,ip	РКСЗ.1: п.17.4 "Условия исключения скрытых каналов", п.3 "Дискреционное управление доступом", п.4 "Мандатное управление доступом и мандатный контроль целостности", п.7.1 "Изоляция процессов", п.8.1 "Очистка памяти", п.16.2 "Киоск-2", п.16.4.11 "Блокировка запуска программ пользователя"
17	ЗИС. 17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы		+	Организационно-технические мероприятия, МЭ	Разбиение информационной системы на сегменты может быть обеспечено с использованием штатных средств Astra Linux, реализующих технологию виртуальных локальных сетей (VLAN) стандарта IEEE 802.1q, а также с использованием средств организации домена.	VLAN	https://wiki.astralinux.ru/x/8w0AB (VLAN)

18	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения			Средства Astra Linux, Организационно-технические мероприятия	Обеспечение загрузки и исполнения программного обеспечения и контроль целостности программного обеспечения осуществляется средствами управления доступом к подключаемым устройствам и средствами контроля целостности (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")) .	Средства разграничения доступа к подключаемым устройствам, Контроль целостности (Afick), ЗПС	РА.1: п.17 "Средства разграничения доступа к подключаемым устройствам" РКСЗ.1: п.16 "Ограничение программной среды", доп: п.16.4.21 "Включение на файловой системе режима работы "только чтение" https://wiki.astralinux.ru/x/HAKtAg (Съемные носители в Astra Linux) https://wiki.astralinux.ru/x/HAKtAg (Съемные USB-носители) https://wiki.astralinux.ru/x/6oR0Ag (Режим замкнутой программной среды) Справка Astra Linux по работе с утилитой управления политикой безопасности fly-admin-smc
19	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			Средства Astra Linux	Изоляция процессов (выполнение программ) в выделенной области памяти реализована в ядре Astra Linux.	Изоляция процессов	РКСЗ.1: п.7 "Изоляция процессов"
20	ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	+	+	Организационно-технические мероприятия, ОРД, Средства Astra Linux	Ограничение на использование в информационной системе беспроводных соединений реализуется средствами Astra Linux, обеспечивающими контроль использования технологий беспроводного доступа на основе	Санкции PolicyKit-1, дискреционное управление доступом, управление драйверами/устройствами	РКСЗ.1: п.3 "Дискреционное управление доступом" https://wiki.astralinux.ru/x/Rg1RBg (Блокировка устройств) Справка Astra Linux по работе программой

						установленной администратором политики выполнения привилегированных действий, дискреционного разграничения доступом и управления устройствами.		управления санкциями PolicyKit-1
21	ЗИС.21	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			Средства Astra Linux	Исключение возможности хранения временных файлов и несанкционированных действий с ними, а также доступа пользователя к «остаточной» информации реализуется с использованием механизмов очистки оперативной и внешней памяти (механизм очистки освобождаемой внешней памяти доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")) и встроенного в ядро Astra Linux механизма изоляции процессов.	Ядро - механизм очистки памяти (astra-secdel-control), механизм очистки разделов подкачки (astra-swapwiper-control), изоляция процессов	РКСЗ.1: п.7 "Изоляция процессов", п.8 "Защита памяти", п.16.4.29 "Управление безопасным удалением файлов", п.16.4.30. "Управление очисткой разделов подкачки"
22	ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы		+	Организационно-технические мероприятия, Средства Astra Linux	Обеспечение защиты от угроз, направленных на отказ в обслуживании, реализуется настройкой режима «киоск», ограничением пользователей по использованию вычислительных ресурсов, интерпретаторов, макросов и консолей, и, для обеспечения усиленной защиты, обеспечением замкнутой программной среды (режим ЗПС доступен для уровней защищенности Astra Linux "Усиленный" ("Воронеж") и "Максимальный" ("Смоленск")).	Режим киоска, ограничивающие функции безопасности (механизмы защиты и блокировок) Дополнительно: ЗПС	РКСЗ.1: п.16 "Ограничение программной среды" https://wiki.astralinux.ru/x/LoKhAQ (Настройка механизмов защиты и блокировок) https://wiki.astralinux.ru/x/zQC4B (Режим киоска)

23	ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями		+ 1, 2, 3, 4а, 4б, 4в, 5	Организационно-технические мероприятия, МЭ, средства однонаправленной передачи, криптошлюзы			-
24	ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения		+	Организационно-технические мероприятия, Средства Astra Linux, Прикладное ПО	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности обеспечивается применением средств организации домена, а также использованием сетевых и прикладных сервисов из состава Astra Linux	Средства организации ЕПП (FreeIPA,ALD, Samba), Защищенный комплекс программ гипертекстовой обработки данных (Apache2), СУБД, Защищенный комплекс программ печати и маркировки документов (cups)	РА.1: п.10 "Защищенный комплекс программ гипертекстовой обработки данных", п.12 "Защищенный комплекс программ печати и маркировки документов" ОП: п.4.1.3 "Организация ЕПП" РА.1: п.8 "Средства организации ЕПП" РА.2 https://wiki.astralinux.ru/x/e4GhAQ (ALD) https://wiki.astralinux.ru/x/X4OhAQ (FreeIPA) https://wiki.astralinux.ru/x/RIImAg (Samba AD и Windows AD)
25	ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного			Организационно-технические мероприятия, Средства Astra Linux, Средства виртуализации	Возможность использования в информационной системе различных типов программного обеспечения реализуется с помощью использования виртуальной инфраструктуры, в составе которой возможно функционирование «недоверенных» гостевых операционных систем в доверенной	Средства виртуализации	РКСЗ.1: п.5 "Защита среды виртуализации" https://wiki.astralinux.ru/x/cQIy (Работа с виртуализацией)

		обеспечения (создание гетерогенной среды)				среде Astra Linux		
26	ЗИС. 26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем			Сторонние средства (ПО «клиент-серверной» архитектуры («тонкого» клиента), имеющих возможность функционирования в средах различных операционных систем)	-	-	-
27	ЗИС. 27	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации			Средства создания ложных информационных объектов,МЭ	-	-	-
28	ЗИС. 28	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных			Средства создания ложных информационных объектов,МЭ	-	-	-

		характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы						
29	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			Организационные мероприятия, Средства Astra Linux	В случае возникновения отказов перевод информационной системы в заранее определенную конфигурацию осуществляется с использованием средств восстановления Astra Linux и с применением наборов базовых конфигураций.	Средства резервного копирования (Bacula, dd, tar, luckybackup, rsync), Резервирование в домене (ALD, FreeIPA), средства управления конфигурациями (Ansible/Puppet/Foreman)	РА.1: п.16 "Резервное копирование и восстановление данных", п.8.3.8.1 "Создание резервной копии и восстановление", п.8.2.6.9 "Создание резервного сервера ALD", п.6.11 "Средство удаленного администрирования Ansible" https://wiki.astralinux.ru/x/dQHGAg (BACULA) https://wiki.astralinux.ru/x/roh0Ag (Архивирование и восстановление файлов с сохранением мандатных атрибутов)
30	ЗИС. 30	Защита мобильных технических средств,	+	+	Средства Astra Linux, Организационные мероприятия	Защита реализуется в зависимости от мобильного технического средства (типа мобильного технического средства) мерами по идентификации	Средства разграничения доступа к подключаемым устройствам, Средства затирания данных (dd, shred)	РА.1: п.17 "Средства разграничения доступа к подключаемым устройствам"

		применяемых в информационной системе				и аутентификации в соответствии с ИАФ.1 и ИАФ.5, управлению доступом в соответствии с УПД.2, УПД.5, УПД.13 и УПД.15, ограничению программной среды в соответствии с ОПС.3, защите машинных носителей информации в соответствии с ЗНИ.1, ЗНИ.2, ЗНИ.4, ЗНИ.8, регистрации событий безопасности в соответствии с РСБ.1, РСБ.2, РСБ.3 и РСБ.5, контролю (анализу) защищенности в соответствии с АНЗ.1, АНЗ.2 и АНЗ.3, обеспечению целостности в соответствии с ОЦЛ.1.		https://wiki.astralinux.ru/x/HAKtAg (Съемные носители в Astra Linux)
XI. Защита среды виртуализации (ЗСВ)								
1.	ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+ 1	Средства Astra Linux	Идентификация и аутентификация пользователей осуществляется с использованием встроенных в ОС СН механизмов идентификации и аутентификации пользователей согласно ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 и ИАФ.7 с учетом требований ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения». Доступ к серверу виртуализации libvirt для управления средствами виртуализации и доступ непосредственно к рабочему столу виртуальной машины при их локальном и удаленном обращении осуществляется только после прохождения процессов идентификации и аутентификации субъектов доступа в ОС СН. Взаимная идентификация и аутентификация пользователей и средства виртуализации при удаленном доступе возможна с использованием удаленной SSH-	Защита среды виртуализации (идентификация и аутентификация пользователей при доступе к виртуальной инфраструктуре), Средства виртуализации (KVM, QEMU, libvirt), средства управления виртуализацией (virt-manager, virsh), Контроль исполняемых файлов (ЗПС), Контроль расширенных атрибутов (ЗПС), Механизм контроля целостности в средстве виртуализации «отпечаток конфигурации»	РКСЗ.1: п.5.4 "Идентификация и аутентификация пользователей в среде виртуализации", п.5.5 "Доверенная загрузка виртуальных машин", п.5.6 "Контроль целостности в среде виртуализации". РА.1: п.9.1.7 "Идентификация и аутентификация при доступе к серверу виртуализации libvirt" РА.1: п.9.1.8 "Идентификация и аутентификация при доступе к рабочему столу виртуальных машин", п. 9.1.10 "Доверенная загрузка виртуальных машин", п. 9.1.11 "Контроль целостности в среде

						аутентификации, а также с использованием сетевого протокола сквозной доверенной аутентификации в ЕПП (удаленная SASL аутентификация с поддержкои□ Kerberos). Аутентификация объектов доступа в виртуальной инфраструктуре, запускаемых и исполняемых модулей программного обеспечения виртуальной инфраструктуры реализуется с использованием: - механизма контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на исполнение; - механизма контроля целостности файлов при их открытии на основе ЭП в расширенных атрибутах файловой системы; - механизма контроля целостности средства виртуализации «отпечаток конфигурации».		виртуализации" Справочный центр: https://wiki.astralinux.ru/x/cQIy (Виртуализация QEMU/KVM в Astra Linux)
2.	ЗСВ. 2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+ 1, 2	+ 1, 2	Средства Astra Linux	Работа в среде виртуализации libvirt подчиняется правилам дискреционного управления доступом и возможна только после прохождения обязательной процедуры идентификации и аутентификации. Монитор обращений контролирует доступ к средствам управления виртуальной инфраструктурой, виртуальным машинам (ВМ), файлам-образам ВМ, виртуальному аппаратному обеспечению, к гипервизору и служебным данным. Дискреционное управление доступом при работе с сервером виртуализации libvirt осуществляется драйвером доступа parsec, специально	Средства виртуализации (KVM, QEMU, libvirt), Защита среды виртуализации (драйвер дискреционного управления доступом parsec, драйвер ролевого управления polkit), средства управления виртуализацией (virt-manager, virsh)	РКСЗ.1: п.5.1 "Дискреционное и ролевое управление доступом в среде виртуализации", п.5.3 "Режим «только чтение»: запрет модификации образа виртуальной машины" РА.1: п.9.1.9 "Ролевое управления доступом" Справочный центр: https://wiki.astralinux.ru/x/cQIy (Виртуализация QEMU/KVM в Astra Linux)

						разработанным с использованием прикладного программного интерфейса драйверов доступа libvirt. Основанием для принятия решения о предоставлении доступа к ВМ является сравнение дискреционных атрибутов ВМ и дискреционных атрибутов пользователя с учетом выполняемой операции и режима запуска ВМ. Также в средстве виртуализации реализован механизм ролевого управления доступом, который базируется на совместном применении драйвера доступа parsec и драйвера доступа Polkit, обеспечивающего разграничение возможностей выполнения привилегированных операций с объектами виртуализации. Управление доступом в виртуальной инфраструктуре осуществляется согласно УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12.		
3.						В режиме ОС СН "Максимальный" работа в среде виртуализации libvirt подчиняется правилам как дискреционного, так и мандатного управления доступом и возможна только после прохождения обязательной процедуры идентификации и аутентификации. Монитор обращений контролирует доступ к средствам управления виртуальной инфраструктурой, виртуальным машинам (ВМ), файлам-образам ВМ, виртуальному аппаратному обеспечению, к	Средства виртуализации (KVM, QEMU, libvirt), Защита среды виртуализации (драйвер дискреционного и мандатного управления доступом parsec, драйвер ролевого управления polkit), средства управления виртуализацией (virt-manager, virsh)	РКСЗ.1: п.5.1 "Дискреционное и ролевое управление доступом в среде виртуализации", п.5.2 "Мандатное управление доступом в среде виртуализации", п.5.3 "Режим «только чтение»: запрет модификации образа виртуальной машины" РА.1: п.9.1.9 "Ролевое

						гипервизору и служебным данным. Дискреционное и мандатное управление доступом при работе с сервером виртуализации libvirt осуществляется драйвером доступа parsec, специально разработанным с использованием прикладного программного интерфейса драйверов доступа libvirt. Также в средстве виртуализации реализован механизм ролевого управления доступом, который базируется на совместном применении драйвера доступа parsec и драйвера доступа Polkit, обеспечивающего разграничение возможностей выполнения привилегированных операций с объектами виртуализации. Управление доступом в виртуальной инфраструктуре осуществляется согласно УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12.		управления доступом" Справочный центр: https://wiki.astralinux.ru/x/cQIy (Виртуализация QEMU/KVM в Astra Linux)
4.	ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	Средства Astra Linux	Регистрация событий безопасности в виртуальной инфраструктуре осуществляется согласно РСБ.1, РСБ.2, РСБ.3, РСБ.4 и РСБ.5. Сбор, запись и хранение информации о событиях безопасности осуществляются подсистемой регистрации событий ОС СН (службой auditd, модулем фильтрации и обработки syslog-ng-mod-astra с участием демона libvirtd). Регистрация осуществляется согласно заданным правилам в системные журналы в каталогах /var/log/ и /var/log/audit/, а также в защищенный журнал /parsec/log/astra/events/. Определение перечня событий,	Средства виртуализации (демон libvirtd), Средства аудита (syslog-ng-mod-astra, auditd, zabbix), Средства просмотра журналов (fly-event-viewer, ksystemlog), Средства управления протоколированием (fly-admin-events, fly-admin-smc, system-config-audit), Центр уведомлений (fly-notifications)	РКСЗ.1: п.5.7 "Регистрация событий безопасности в среде виртуализации" РА.1: п.9.1.12 "Регистрация событий в среде виртуализации", п.16 "Средства аудита и централизованного протоколирования" Справочный центр: https://wiki.astralinux.ru/x/-4JOAg (Zabbix)

						необходимых для регистрации и учета, выполняется с использованием утилиты fly-admin-events («Настройка регистрации системных событий»). Просмотр и анализ журналов событий безопасности осуществляется администратором с использованием консольных инструментов (ausearch, aureport, aulast, auvirt, journalctl) и графических утилит fly-event-viewer (просмотр журнала /parsec/log/astra/events) и ksystemlog. Информирование администратора о событиях безопасности осуществляется с использованием «Центра уведомлений» (fly-notifications). Реагирование системы на события безопасности задается с использованием утилиты «Настройка регистрации системных событий» (fly-admin-events). Для решения задач централизованного протоколирования и анализа журналов аудита, а также организации распределенного мониторинга сети, жизнеспособности и целостности серверов используется программное решение Zabbix.		
5.	ЗСВ. 4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами		+	Средства Astra Linux, МЭ, СКЗИ	Для управления потоками информации в виртуальной инфраструктуре на канальном и сетевом уровнях применяются следующие встроенные механизмы управления потоками ОС СН, обеспечивающие сетевую фильтрацию того или иного типа: - драйвер виртуальных сетей libvirt (обеспечивает изолированное мостовое устройство, к которому	Средства виртуализации (KVM, QEMU, libvirt), Защита среды виртуализации (драйвер виртуальных сетей libvirt, драйвер сетевых фильтров nwfilter), VLAN, Open vSwitch, средства управления виртуализацией (virt-manager, virsh) Дополнительно: Сертифицированные МСЭ	РКС3.1: п.5.9 "Управление потоками информации в среде виртуализации" РА.1: п.9.1.14 "Управление потоками информации в среде виртуализации", п.6.8 "Программный коммутатор Open vSwitch"

		виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				подключены гостевые TAP-устройства, возможна работа в режимах isolated, NAT, forward); - драйвер сетевых фильтров libvirt (обеспечивает полностью настраиваемую сетевую фильтрацию трафика на гостевых сетевых адаптерах с использованием сетевых фильтров nwfilter); - изоляция сетей с помощью VLAN (с применением программного многоуровневого коммутатора Open vSwitch). Для реализации меры использование только штатных средств может быть недостаточно. При построении виртуальных инфраструктур рекомендуется применение совместимых с ОС СН сертифицированных МСЭ		Справочный центр: https://wiki.astralinux.ru/x/jJJYDw (Межсетевые экраны в среде виртуализации Astra Linux)
6.	ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			Средства Astra Linux, СДЗ	Доверенная загрузка виртуальных машин обеспечивается: - с использованием механизма контроля целостности файлов при их открытии на основе ЭЦП (режим ЗПС) для обеспечения динамического контроля целостности конфигурации виртуального оборудования виртуальных машин, параметров настройки средства виртуализации и файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины); - с использованием механизма запрета запуска исполняемых файлов и разделяемых библиотек с неверной ЭЦП, а также без ЭЦ (режим ЗПС) для контроля целостности исполняемых файлов средства виртуализации; - с использованием механизма	Контроль исполняемых файлов (ЗПС), Контроль расширенных атрибутов (ЗПС), Защита среды виртуализации (механизм контроля целостности в средстве виртуализации «отпечаток конфигурации»)	РКСЗ.1: п.5.5 "Доверенная загрузка виртуальных машин" РА.1: п.9.1.10 "Доверенная загрузка виртуальных машин"

						контроля целостности средства виртуализации «отпечаток конфигурации», осуществляющего динамический контроль целостности конфигурации виртуального оборудования виртуальных машин, параметров настройки средства виртуализации и файлов виртуальной базовой системы ввода-вывода. При выявлении нарушения целостности объектов контроля осуществляется блокировка их запуска. Для обеспечения доверенной загрузки ЭВМ необходимо использовать средства доверенной загрузки или аппаратно-программные модули доверенной загрузки.		
7.	ЗСВ. 6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		+ 1	Организационные мероприятия, Средства Astra Linux	Средства виртуализации из состава ОС СН поддерживает возможность миграции виртуальных машин с одного физического хоста на другой без остановки ее работы. Управление перемещением виртуальных машин реализуется с использованием интерфейсов управления средствам виртуализации Libvirt в соответствии с установленными правилами сетевого взаимодействия. В среде виртуализации реализовано создание, модификация, хранение, получение и удаление (в т.ч. централизованное) образов виртуальных машин. Для централизованного хранения образов ВМ используются хранилища данных, построенные на базе кластерной файловой системы ocfs2 или блочных устройств ceph/rbd.	Средства виртуализации (KVM, QEMU, libvirt), средства управления виртуализацией (virt-manager, virsh), Защита среды виртуализации (механизм централизованного хранения образов ВМ, механизм миграции ВМ)	РКСЗ.1: п.5.12 "Централизованное управление образами виртуальных машин и виртуальными машинами" РА.1: п.9.1.16 "Централизованное управление"
8.	ЗСВ. 7	Контроль целостности		+ 3	Средства Astra Linux	Контроль целостности виртуальной инфраструктуры и ее конфигураций	Контроль исполняемых файлов (ЗПС), Контроль	РКСЗ.1: п.5.6 "Контроль целостности в среде

		виртуальной инфраструктуры и ее конфигураций				реализуется: - с использованием механизма контроля целостности файлов при их открытии на основе ЭЦП (режим ЗПС) для обеспечения динамического контроля целостности конфигурации виртуального оборудования виртуальных машин, параметров настройки средства виртуализации и файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины); - с использованием механизма запрета запуска исполняемых файлов и разделяемых библиотек с неверной ЭЦП, а также без ЭЦ (режим ЗПС) для контроля целостности исполняемых файлов средства виртуализации; - с использованием механизма контроля целостности средства виртуализации «отпечаток конфигурации», осуществляющего динамический контроль целостности конфигурации виртуального оборудования виртуальных машин, параметров настройки средства виртуализации и файлов виртуальной базовой системы ввода-вывода; - с использованием механизм регламентного контроля целостности AFICK.	расширенных атрибутов (ЗПС), Защита среды виртуализации (механизм контроля целостности в средстве виртуализации «отпечаток конфигурации»), средства регламентного контроля целостности AFICK	виртуализации", п.9 "Контроль целостности", п.16.1. "Замкнутая программная среда" РА.1: п. 9.1.11 "Контроль целостности в среде виртуализации"
9.	ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной		+	Организационно-технические мероприятия, Средства Astra Linux	Резервное копирование образов виртуальных машин и конфигурации виртуального оборудования виртуальных машин, а также параметров настройки средств виртуализации и сведений о событиях безопасности реализуется с использованием встроенных в средства виртуализации ОС СН	Защита среды виртуализации (механизмы резервного копирования средства виртуализации virsh backup-begin, virsh dumpxml, virsh snapshot-create), Средства резервного копирования (Bacula, dd, tar, luckybackup, rsync), Средства обеспечения	РКСЗ.1 п.5.8 "Резервное копирование в среде виртуализации", п.10 "Надежное функционирование" РА.1: п.7 "Средства обеспечения отказоустойчивости и высокой доступности",

		инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры				механизмов резервного копирования (инструментов командной строки virsh backup-begin, virsh dumpxml и virsh snapshot-create), а также встроенных в ОС СН средств резервного копирования, средств кластеризации и создания распределенных хранилищ информации, механизмов агрегации каналов.	отказоустойчивости и высокой доступности (Ceph, OCFS2, bounding)	п.9.1.13 "Резервное копирование в среде виртуализации", п.17 "Резервное копирование и восстановление данных" Справочный центр: https://wiki.astralinux.ru/x/uhx0CQ (Механизмы агрегации сетевых каналов)
10	ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+ 1	САВЗ	Реализуется сертифицированными САВЗ	-	-
11	ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	+	+	Организационно-технические мероприятия, Средства Astra Linux	Разбиение виртуальной инфраструктуры на сегменты может быть обеспечено с использованием штатных средств ОС, реализующих технологию виртуальных локальных сетей (VLAN) стандарта IEEE 802.1q, с применением программного многоуровневого коммутатора Open vSwitch, а также драйвера виртуальных сетей libvirt и драйвера сетевых фильтров nwfilter. Сегментирование виртуальной инфраструктуры может также выполняться путем организации единого пространства пользователей (ЕПП), в основу которого положен доменный принцип построения сети с использованием сетевого протокола сквозной доверенной аутентификации. Изоляция потоков данных в виртуальной инфраструктуре обеспечивается использованием технологии KVM, которая включает специальный	VLAN, Open vSwitch, Защита среды виртуализации (драйвер виртуальных сетей libvirt, драйвер сетевых фильтров nwfilter), Средства организации ЕПП Дополнительно: Сертифицированные МСЭ	РКСЗ.1: п.5.9 "Управление потоками информации в среде виртуализации" РА.1: п.9.1.14 "Управление потоками информации в среде виртуализации", п.6.8 "Программный коммутатор Open vSwitch" Справочный центр: https://wiki.astralinux.ru/x/8w0AB (VLAN)

						модуль ядра и средство создания виртуального аппаратного окружения для изоляции и управления виртуальными гостевыми машинами. Изоляция процессов (выполнение программ) в выделенной области памяти реализована в ядре ОС. При построении виртуальных инфраструктур рекомендуется применение совместимых с ОС СН сертифицированных МСЭ: https://wiki.astralinux.ru/x/jJJYDw		