Согласовано ФСТЭК России
от 31.01.2024 г

Методические рекомендации по безопасной настройке операционной системы специального назначения «Astra Linux Special Edition»

Изменение 1

(Листов - 123)

Москва
2024

СОДЕРЖАНИЕ

АННОТАЦИЯ

Настоящий документ содержит общие рекомендации по настройке безопасных конфигураций параметров безопасности операционной системы специального назначения «Astra Linux Special Edition» очередного обновления 1.8 (далее по тексту — ОС), применяемой для реализации мер защиты информации в государственных информационных системах, информационных системах персональных данных, значимых объектов критической информационной инфраструктуры.

Целью выполняемых в соответствии с настоящим документом настроек является обеспечение состояния защищенности ОС, которое достигается системой мероприятий:

1. Выполнением указаний по обеспечению безопасности среды функционирования ОС, согласно разделу 2 настоящего методического документа.

2. Выполнением указаний по установке, обновлению и резервному копированию ОС, согласно разделу 3 настоящего методического документа.

3. Применением конфигурации параметров безопасности, согласно разделу 4 настоящего методического документа.

Рекомендации направлены на повышение защищенности информационных (автоматизированных) систем, функционирующих под управлением ОС, обеспечение мер защиты информации и нейтрализации актуальных угроз безопасности информации, которые могут быть реализованы с использованием некорректных конфигураций ОС.

Настройка ОС осуществляется в соответствии с эксплуатационной документацией.

1. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СРЕДЫ ФУНКЦИОНИРОВАНИЯ ОС

1.1. Использование средств доверенной загрузки

В целях обеспечения безопасности среды функционирования ОС должна быть обеспечена доверенная загрузка ОС. Доверенную загрузку ОС рекомендуется выполнять с помощью сертифицированных средств доверенной загрузки или модулей доверенной загрузки. При технической невозможности или нецелесообразности использования таких средств должны быть приняты организационно-технические меры, предотвращающие возможность доступа пользователя к ресурсам СВТ в обход механизмов защиты ОС (должна отсутствовать возможность загрузки альтернативной операционной системы на средства вычислительной техники (далее — СВТ) и модификации модулей загружаемой ОС).

После установки ОС согласно документации на средство доверенной загрузки следует установить единственным устройством для загрузки ОС жесткий диск, на который произведена установка ОС.

Для обеспечения невозможности отключения функций защиты ОС необходимо обеспечить контроль целостности критически важных компонент системы (загрузчик, ядро ОС, файлы конфигураций) средствами доверенной загрузки до ее загрузки.

Таблица 1.1 - Рекомендации по контролю целостности средством доверенной загрузки

№	Объект контроля целостности	Примечание
1.	Главная загрузочная запись (MBR)	Контролировать целостность MBR необходимо для носителя информации, на который устанавливается защищаемая ОС, если в эту область записывается загрузчик.
2.	Загрузочный сектор раздела (PBR)	Контролировать целостность PBR необходимо в случае, если в него записывается часть загрузчика ОС GNU/Linux при установке (вместо MBR).
3.	Сектора 1-63 относительно начала загрузочного раздела	Контролировать целостность данных секторов необходимо в случае, если часть загрузчика записывается в эту область (например, загрузчик grub записывает в указанные сектора свои компоненты).

№	Объект контроля целостности	Примечание
4.	Раздел ESP	Контролировать целостность данного раздела необходимо в случае использования таблицы разделов GPT, если EFI-загрузчик размещается в разделе ESP (имеет имя /EFI/Boot/bootx64.efi).
5.	/boot/vmlinuz-*	Файлы образов ядра ОС.
6.	/boot/initrd.img-*	Файлы образов временной файловой системы, используемой ядром ОС при начальной загрузке (добавляются в список контроля целостности после выполнения всех необходимых операций по настройке, требующих обновления образов временной файловой системы).
7.	/boot/grub/grub.cfg	Конфигурационный файл меню загрузчика GRUB 2.
8.	/boot/grub/*	Файлы модульной структуры GRUB 2.
9.	/lib/modules/*/misc/digsig_verif.ko /lib/modules/*/misc/parsec.ko /lib/modules/*/misc/parsec-cifs.ko	Модули безопасности подсистемы PARSEC, включая модули обеспечения замкнутой программной среды ОС.
10.	/etc/astra_license /etc/nsswitch.conf /etc/pam.d/fly-dm /etc/pam.d/fly-dm-np /etc/pam.d/login /etc/pam.d/passwd /etc/pam.d/su /etc/pam.d/sumac.xauth /etc/pam.d/xrdp-sesman	Конфигурационные файлы, влияющие на загрузку критически важных функций безопасности.

Постановка на контроль средствами доверенной загрузки файлов конфигурации и критичных данных ОС (например, /etc/fstab, /etc/pam.d/*, /etc/parsec/* и др.) должна осуществляться в зависимости от целей и функциональных задач применения ОС: если данные компоненты планируется подвергать частой санкционированной модификации в процессе эксплуатации – для их контроля целесообразно ограничиться средствами контроля целостности из состава ОС.

1.2. Защита BIOS

Необходимо выполнить установку пароля на BIOS в настройках согласно документации. Защита паролем BIOS может предотвратить несанкционированный доступ внутренних нарушителей к защищаемым данным, имеющих физический доступ к компьютеру.

Рекомендуемые характеристики пароля: длина пароля не менее восьми символов, алфавит пароля не менее 70 символов.

При наличии опций для процессоров Intel Execute Disable Bit (XD-Bit) и для процессоров AMD No Execute Bit (NX-Bit) - включить их.

1.3. Защита СВТ

Должна быть обеспечена защита от осуществления действий, направленных на нарушение физической целостности СВТ, на котором функционирует ОС. Рекомендуется обеспечить защиту от «незаметного» вскрытия корпуса и встраивания «имплантов» в соединительные кабели периферийных устройств. Для обеспечения защиты могут использоваться специальные корпуса, защитные крышки, пломбы, пломбировочные ленты, для усложнения скрытной установки «имплантов» рекомендуется использование СВТ в форм-факторе ноутбук или моноблок.

Рекомендуется обеспечить защиту от скачков электронапряжения, выполнение норм и правил устройства и технической эксплуатации электроустановок, соблюдение параметров электропитания и заземления технических средств. Для обеспечения защиты могут использоваться сетевые фильтры, стабилизаторы или устройства бесперебойного электропитания.

Рекомендуется отключить (физически) непланируемые к использованию проводные и беспроводные периферийные устройства ввода/вывода (мыши, клавиатуры, «тачпады», микрофоны, видеокамеры и пр.).

1.4. Защита сетевого взаимодействия

Перед подключением к сетям общего пользования необходимо обеспечить общие настройки сетевого взаимодействия:

– назначить IP –адрес;

– назначить широковещательный адрес и связанную с ним маски подсети;

– включить сетевой интерфейс;

– проверить таблицу маршрутизации;

– ограничить доступ к внешним адресам и доменам.

В ОС поддерживаются следующие возможные способы настройки сети:

– с использованием службы NetworkManager. Эта служба в первую

очередь предназначена для использования на персональных компьютерах, предоставляет удобный графический интерфейс для выполнения базовых операций, но потребляет довольно много ресурсов, поэтому для серверных приложений не рекомендуется. Помимо проводных сетевых интерфейсов может работать с интерфейсами Wi-Fi. При стандартной установке ОС служба NetworkManager и соответствующий графический инструмент устанавливаются и запускаются автоматически, получая под свое управление все внешние сетевые интерфейсы.

– с использованием службы networking / resolvconf. Служит для автоматизации настроек сетевых интерфейсов и (при использовании пакета resolvconf) для автоматизации перенастройки службы DNS при переключении между сетями. Удобна для использования в сценариях для автоматизации сложных серверных конфигураций. При стандартной установке Astra Linux служба networking устанавливается и запускается автоматически, однако управление имеющимися внешними сетевыми интерфейсами автоматически не получает, и формально управляет только интерфейсом локальной обратной петли (loopback). С использованием службы выполняется традиционная настройка сети TCP/IP из командной строки с использованием инструментов ifup и ifdown. Работает с сетевыми интерфейсами, перечисленными в файле /etc/network/interfaces. При переходе к использованию службы networking следует отключить NetworkManager (в том числе для избегания возможных конфликтов в части управления /etc/resolv.conf).

– с использованием служб systemd-networkd / systemd-resolved, служащих для автоматизации настроек сетевых интерфейсов и правил разрешения имён, базирующиеся на идеологии systemd. При стандартной установке ОС эти службы устанавливаются автоматически, однако находятся в заблокированном состоянии, соответственно, не запускаются, и ничем не управляют.

– с использованием службы connman — служба и интерфейс командной строки для управления сетями в мобильных устройствах.

При необходимости выполняется отключение автоматического конфигурирования сети с использованием инструмента astra-noautonet-control. Инструмент astra-noautonet-control блокирует автоматическое конфигурирование сетевых подключений путем блокировки работы служб NetworkManager, network-manager и connman, а также выключает отображение элемента управления сетевыми подключениями в области уведомлений панели задач. Данная блокировка обеспечивает предотвращение нарушений работы сети в случае появления в сети неправильно настроенного сервера DHCP, некорректно отвечающего на запросы клиентов.

Ограничение доступа к внешним адресам и доменам осуществляется путем явного задания в файлах /etc/hosts.allow и /etc/hosts.deny разрешенных и запрещённых протоколов, IP-адресов и DNS-имен.

По решению администратора об использовании встроенных механизмов фильтрации сетевых потоков в качестве дополнительной меры по защите информации выполняется настройка встроенного межсетевого экрана с использованием консольных средств ufw и iptables или в графическом режиме с использованием gufw («Пуск» - «Параметры» - раздел «Безопасность» - «Межсетевой экран» - «Настройка межсетевого экрана») в минимально необходимой конфигурации, необходимой для работы: по умолчанию все запрещено, кроме необходимых исключений.

При организации сетевого взаимодействия необходимо обеспечить доверенный канал передачи информации между СВТ, на которых установлена ОС, обеспечить контроль несанкционированного подключения к локально-вычислительным сетям в пределах контролируемой зоны, обеспечить защищенную передачу сетевого трафика за пределами контролируемой зоны. Обеспечение защиты информации при межсетевом доступе (через внешние информационно-телекоммуникационные сети) реализуется сертифицированными криптографическими средствами защиты в соответствии с законодательством Российской Федерации.

В случае наличия средств удаленного администрирования и беспроводных систем передачи данных должны быть предприняты меры по нейтрализации возможностей реализации атак и скрытых каналов передачи данных.

2. УКАЗАНИЯ ПО УСТАНОВКЕ, ОБНОВЛЕНИЮ И РЕЗЕРВНОМУ КОПИРОВАНИЮ ОС

2.1. Рекомендации по установке

Выбор уровня защищенности

В графическом режиме при установке ОС на приветственной странице пользователю предлагается выбрать уровень защищенности в зависимости от приобретенной лицензии и принять условия Лицензионного соглашения. Выбор варианта лицензирования обосновывается исходя из результатов анализа возможностей ОС по реализации базовых мер защиты и возможностей по нейтрализации актуальных угроз безопасности информации.

Таблица 2.1 - Общие рекомендации по выбору уровня защищенности

№ п/п	Наименование варианта лицензирования	Описание уровня защищенности
1.	Вариант лицензирования «Орел» (уровень защищенности «Базовый»)	Вариант лицензирования «Орел» может применяться только в системах, не обрабатывающих информацию, подлежащую защите в соответствии с законодательством Российской Федерации.
2.	Вариант лицензирования «Воронеж» (уровень защищенности «Усиленный»)	Усиленный уровень безопасности предназначен для обработки и защиты информации ограниченного доступа, не составляющей государственную тайну, в том числе в ГИС, ИСПД и значимых объектов КИИ любого класса (уровня) защищенности (категории значимости).
3.	Вариант лицензирования «Смоленск (уровень защищенности «Максимальный»)	Уровень максимальной защищенности предназначен для обработки информации любой категории доступа в ГИС, в ИСПД, в составе значимых объектов КИИ, в иных информационных (автоматизированных) системах, обрабатывающих информацию ограниченного доступа, в т.ч. содержащую сведения, составляющие государственную тайну до степени секретности «особой важности» включительно.

Рекомендации по настройке дисковых разделов

Для редактирования схемы разметки диска в разделе «Компоненты установки» графической программы установки необходимо открыть программу разметки диска и перейти к настройкам конфигурации разметки диска.

Высокоуровневые системные каталоги рекомендуется располагать на отдельных физических разделах или логических томах. Общие принципы работы с физическими разделами или томами изложены ниже.

Корневая директория /, а также директории /boot, /tmp, /var, /var/tmp, /parsec, /home рекомендуется выделить в отдельные разделы файловой системы.

Ручная разметка жесткого диска позволяет применить защитное преобразование данных для отдельных дисковых разделов.

Для корректного применения в ОС режима очистки освобождающихся дисковых ресурсов рекомендуется исключить использование дисков SSD для хранения конфиденциальной информации.

Отдельные дисковые разделы создавать в соответствии с рекомендациями, указанными в таблице 2.2.

Таблица 2.2 - Рекомендации на настройке разделов

Раздел	**Описание**	**Рекомендации по установке/настройке**
/	Корневой раздел	Рекомендуется применять защитное преобразование (при условии, что каталог /boot размещён в отдельном дисковом разделе)
/boot	Раздел для хранения образов загрузчика и образов ядра, которые используются для загрузки ОС	Без защитного преобразования. Раздел /boot недопустимо размещать в LVM. Рекомендуется выделить под этот раздел не менее 512МБ, предпочтительно 1GB
/home	Раздел предназначен для хранения пользовательских данных. Создание такого раздела позволяет сохранить данные при переустановке ОС, а также делает удобным частое резервное копирование пользовательских данных	Рекомендуется применять защитное преобразование
/tmp	Разделы /tmp и /var/tmp/ используются для хранения временных пользовательских данных и служебных данных системы	Рекомендуется применять защитное преобразование. При размере раздела /tmp менее 250МБ весьма вероятно возникновение ошибок при работе с графикой или с большими объёмами данных

Раздел	Описание	Рекомендации по установке/настройке
/var	Раздел для хранения данных аудита /var/log, /var/log/audit	Рекомендуется применять защитное преобразование
/var/tmp	Разделы /tmp и /var/tmp/ для хранения временных пользовательских данных и служебных данных системы	Рекомендуется применять защитное преобразование
/parsec	Раздел для хранения журнала событий /parsec/log/astra/events	Рекомендуется применять защитное преобразование
swap	Служебный раздел для хранения временных файлов, создаваемых системой для расширения оперативной памяти. Рекомендуется вместо раздела подкачки использовать файл подкачки	Если необходимо использовать - то использовать с включенным защитным преобразованием и с включенным гарантированным удалением и очисткой разделов страничного обмена в ОС

Установка компонентов

В секции «Компоненты операционной системы» раздела «Компоненты установки» приведены доступные для установки наборы программного обеспечения (ПО). Должна осуществляться инсталляция только того необходимого ПО, которое предназначено для решения конкретных функциональных задач.

В секции «Дополнительные настройки» приведены доступные функции безопасности ОС, а также функции автоматической настройки сети и выбора времени в качестве системного. Список доступных функций безопасности зависит от выбранного уровня защищенности.

Включение функций защиты на данном этапе (этапе установки ОС) осуществляется в соответствии с рекомендациями, указанными в таблице 2.3.

Таблица 2.3 - Рекомендации на настройке функций безопасности

Функция	Описание	Рекомендация
Мандатный контроль целостности	При выборе данного пункта будет включен механизм мандатного контроля целостности. По умолчанию пункт выбран (доступен для усиленного уровня защищенности).	Рекомендуется к включению

Функция	Описание	Рекомендация
Мандатное управление доступом	При выборе данного пункта будет включен механизм мандатного управления доступом. По умолчанию пункт выбран (доступен для максимального уровня защищенности).	Рекомендуется к включению
Замкнутая программная среда	При выборе данного пункта будет включен механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов формата ELF. По умолчанию пункт не выбран (доступен для усиленного уровня защищенности).	Рекомендуется к включению. Допускается настройка и включение после установки и окончательной настройки ОС
Очистка освобождаемой внешней памяти	При выборе данного пункта будет включен режим очистки блоков файловой системы (далее по тексту - ФС) непосредственно при их освобождении, а также режим очистки разделов страничного обмена. По умолчанию пункт не выбран (доступен для усиленного уровня защищенности).	Рекомендуется к включению. Допускается настройка и включение после установки и окончательной настройки ОС
Запрет вывода меню загрузчика	При выборе данного пункта будет запрещен вывод меню загрузчика GRUB 2. В процессе загрузки будет загружаться ядро ОС, выбранное по умолчанию. По умолчанию пункт не выбран.	Рекомендуется к включению. Допускается включение после установки и окончательной настройки ОС
Запрет трассировки ptrace	При выборе данного пункта будет выключена возможность трассировки и отладки выполнения программного кода. По умолчанию пункт выбран.	Рекомендуется к включению. Допускается включение после установки и окончательной настройки ОС
Запрос пароля для команды sudo	При выборе данного пункта будет включено требование ввода пароля при использовании механизма sudo. По умолчанию пункт выбран.	Рекомендуется к включению

Функция	Описание	Рекомендация
Запрет установки бита исполнения	При выборе данного пункта будет включен режим запрета установки бита исполнения, обеспечивающий предотвращение несанкционированного запуска исполняемых файлов и сценариев для командной оболочки. По умолчанию пункт не выбран.	Рекомендуется к включению. Допускается включение после установки и окончательной настройки ОС
Запрет исполнения скриптов пользователя	При выборе данного пункта будет блокировано интерактивное использование пользователем интерпретаторов. По умолчанию пункт не выбран.	Рекомендуется к включению. Допускается включение после установки и окончательной настройки ОС
Запрет исполнения макросов пользователя	При выборе данного пункта будет блокировано исполнение макросов в стандартных приложениях. По умолчанию пункт не выбран.	Рекомендуется к включению. Допускается включение после установки и окончательной настройки ОС
Запрет консоли	При выборе данного пункта будет блокирован консольный вход в систему для пользователя и запуск консоли из графического интерфейса сессии пользователя. По умолчанию пункт не выбран.	Рекомендуется к включению. Допускается включение после установки и окончательной настройки ОС
Системные ограничения ulimits	При выборе данного пункта будут включены системные ограничения, установленные в файле /etc/security/limits.conf. По умолчанию пункт не выбран.	Рекомендуется к включению. Допускается включение после установки и окончательной настройки ОС
Запрет автонастройки сети	При выборе данного пункта будет выключена автоматическая настройка сети в процессе	Рекомендуется к включению

Функция	Описание	Рекомендация
	установки ОС, сеть необходимо будет настроить вручную. По умолчанию пункт не выбран.	
Местное время для системных часов	При выборе данного пункта будет включен режим интерпретации показаний аппаратных (RTC) часов. По умолчанию пункт не выбран.	На усмотрение администратора

Пароль для учетной записи администратора

В разделе «Редактор пользователей» программы установки необходимо задать имя и пароль для учетной записи администратора в соответствии с требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов. Имеется возможность добавления учетных записей и паролей для других пользователей ОС.

Установка пароля на системный загрузчик должна осуществляться в соответствии с требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов.

Рекомендуемые характеристики пароля: длина пароля не менее восьми символов, алфавит пароля не менее 70 символов.

2.2. Настройка ОС согласно указаниям по эксплуатации

Непосредственно после установки ОС и до начала использования компьютера по назначению необходимо произвести настройку параметров безопасности согласно указаниям по эксплуатации, приведенным в эксплуатационной документации ОС («Руководство администратора по КСЗ, Часть 1» п. 18.2).

2.3. Отключение неиспользуемых сервисов и аппаратных устройств

Отключение беспроводных соединений

В случае отсутствия необходимости применения технологий беспроводного доступа обеспечивается исключение возможности осуществления беспроводных подключений следующими настройками:

1) Отключение всех беспроводных интерфейсов, например, путем внесения изменений в файл /etc/network/interfaces и применением команды:

ifdown <наименование интерфейса (например: wlan0, ath0, wifi0)>

2) Отключение устройства, добавив его модуль в blacklist. Так, для блокировки модулей ath9k и btusb, в /etc/modprobe.d/blacklist.conf необходимо внести следующую запись:

blacklist ath9k

blacklist btusb

При последующей перезагрузке устройство перестанет работать.

3) Для исключения подключения других устройств, модули этих устройств можно удалить физически из /lib/modules/<версия_ядра>/kernel/drivers. Например, удалить драйвера беспроводных устройств можно с помощью команды:

rm -r /lib/modules/<версия_ядра>/kernel/drivers/net/wireless

Отключение микрофона и вэб-камеры

Отключение микрофона и вэб-камеры целесообразно обеспечить включением соответствующих драйверов в «черный список» загрузки. Для этого необходимо:

1) Получить наименования нужных драйверов. В частности, драйверов звуковой карты:

cat /proc/asound/modules

2) Включить в конфигурационный файл /etc/modprobe.d/blacklist.conf перечень драйверов, например, для звуковой карты и UVC-устройств:

blacklist snd_hda_intel

blacklist uvcvideo

2.4. Конфигурирование наиболее уязвимых системных служб

Конфигурирование SSH

Конфигурирование параметров, отвечающих за безопасность при удаленном подключении с использованием SSH, обеспечивается настройками конфигурационного файла клиента */etc/ssh/ssh_config,* приведенными в таблице 2.4, и конфигурационного файла сервера */etc/ssh/sshd_config*, приведенными в таблице 2.5.

Таблица 2.4 - Параметры конфигурирования /etc/ssh/ssh_config

№ п/п	Описание настройки	Конфигурируемый параметр
1.	Смена порта по умолчанию	Port <номер>
2.	Настроить тайм-аут подключения к серверу SSH (сек.)	ServerAliveInterval 15
3.	Ограничить количество одновременных подключений до 1	ServerAliveCountMax 1

Таблица 2.5 - Параметры конфигурирования /etc/ssh/sshd_config

№ п/п	Описание настройки	Конфигурируемый параметр
1.	Смена порта по умолчанию	Port <номер>
2.	Запрет удаленного подключения подключаться через SSH от имени root-пользователя	PermitRootLogin no
3.	Указать имена пользователей или групп, которым разрешено подключение к серверу SSH и/или запретить некоторым пользователям (группам) подключение к SSH	AllowUsers <имя_пользователя 1> <имя_пользователя_2> И/Или DenyUsers <имя_пользователя 1> <имя_пользователя_2>

Конфигурирование Samba

Конфигурирование параметров, отвечающих за безопасность функционирования при подключении к сетям общего доступа, обеспечивается настройками файла /etc/samba/smb.conf, приведенными в таблице 2.6.

Таблица 2.6 - Параметры конфигурирования samba

№ п/п	Описание настройки	Конфигурируемый параметр
1.	Отключение гостевой учётной записи и локальной поддержки входа в систему	[share] guest ok = no
2.	Отключение доступа для root	[share] invalid users = root
3.	Установить запрет на подключение по SMB с с внешней сети	[IPC$] hosts allow = <IP>. 127.0.0.1 hosts deny = 0.0.0.0/0
4.	Ограничить совместный доступ к файлам	[share] hosts allow = <IP>. 127.0.0.1 valid users = <имя_пользователя1> <имя_пользователя2>
5.	Запрет совместного доступа к принтеру	Убрать или закомментировать блок [printers]

Конфигурирование встроенного Web-сервера Apache

Конфигурирование параметров, отвечающих за безопасность функционирования при подключении к сетям общего доступа, обеспечивается настройками файла /etc/apache2/apache2.conf, приведенными в таблице 2.7.

Таблица 2.7 - Параметры конфигурирования Apache

№ п/п	Описание настройки	Конфигурируемый параметр
1.	Скрыть версию Apache при сетевом сканировании	ServerSignature Off ServerTokens Prod
2.	Установить запуск Apache от специального пользователя и группы, заданного в /etc/apache2/envvars	User ${APACHE_RUN_USER} Group ${APACHE_RUN_GROUP }
3.	Выключить просмотр директорий	Options -Indexes Options -Includes
4.	Запретить персистентные соединения	KeepAlive Off
5.	Установить таймаут не более 45 сек	Timeout 45
6.	Ограничить запросы с передачей данных более 10 Мб	LimitXMLRequestBody 10485760
7.	Включить обязательную аутентификацию	AstraMode on

2.5. Конфигурирование параметров ядра

Настройка параметров безопасности ядра осуществляется в соответствии с рекомендациями, приведенными в таблице 2.8, путем добавления параметров в конфигурационные файлы sysctl, например, в /etc/sysctl.d/99-sysctl.conf.

После внесения изменений необходимо перезагрузить компьютер и убедиться, что все параметры сохранены правильно.

Сделать проверку можно командой:

sudo sysctl -a | more

Таблица 2.8 - Рекомендуемые значения параметров конфигурировании ядра

№ п/п	Описание настройки	Конфигурируемый параметр
1.	Отключение переадресации IP пакетов. Рекомендуется выполнять на узлах, не выполняющих маршрутизацию	net.ipv4.ip forward=0 net.ipv6.conf.all.forwarding=0 net.ipv6.conf.default.forwarding=0
2.	Параметры, отвечающие за выдачу ICMP Redirect (ICMP перенаправления) другим хостам. Рекомендуется выполнять на узлах, не выполняющих маршрутизацию	net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.all.secure_redirects=0 net.ipv4.conf.all.send_redirects=0 net.ipv4.conf.default.accept_redirects=0 net.ipv4.conf.default.secure_redirects=0 net.ipv4.conf.default.send_redirects=0

№ п/п	Описание настройки	Конфигурируемый параметр
		net.ipv6.conf.all.accept_redirects=0 net.ipv6.conf.default.accept_redirects=0 net.ipv6.conf.all.accept_ra=0 net.ipv6.conf.default.accept_ra=0
3.	Если IPv6 не используется, то его рекомендуется отключить	net.ipv6.conf.all.disable_ipv6=1 net.ipv6.conf.default.disable_ipv6=1 net.ipv6.conf.lo.disable_ipv6=1
4.	Ограничение небезопасных вариантов работы с жесткими ссылками (hardlinks)	fs.protected_hardlinks = 1
5.	Ограничение небезопасных вариантов прохода по символическим ссылкам (symlinks)	fs.protected_symlinks = 1
6.	Запрет создания core dump для некоторых исполняемых файлов	fs.suid_dumpable=0
7.	Рандомизация адресного пространства, которая защищает от атак на переполнение буфера	kernel.randomize_va_space=2
8.	Использование фильтрации обратного пути по умолчанию. Не рекомендуется в случае использования несимметричной маршрутизации	net.ipv4.conf.default.rp_filter=1
9.	Использование фильтрации обратного пути у всех интерфейсов. Не рекомендуется в случае использования несимметричной маршрутизации	net.ipv4.conf.all.rp_filter=1
10.	Ограничение доступа к журналу ядра	kernel.dmesg_restrict=1
11.	Запретить подключение к другим процессам с помощью ptrace	kernel.yama.ptrace_scope=3
12.	Инициализация динамической ядерной памяти нулем при ее выделении	init_on_alloc = 1
13.	Включение средств защиты от аппаратных уязвимостей центрального процессора	mitigations=auto
14.	Ограничение доступа к событиям производительности	kernel.perf_event_paranoid = 4
15.	Запрет системного вызова userfa ultfd для непривилегированных пользователей	vm.unprivileged_userfaultfd = 0
16.	Настройка параметра ядра, определяющего минимальный виртуальный адрес, который процессу разрешено использовать для mmap.	vm.mmap_min_addr = 65536

№ п/п	Описание настройки	Конфигурируемый параметр
	Значение должно быть больше 4096	

2.6. Рекомендации по обновлению

Администратором безопасности осуществляется получение из доверенных источников, анализ, принятие решения по установке и установка очередных и внеочередных обновлений ОС.

Предварительно администратором выполняется проверка возможности восстановления ОС из резервной копии (включая восстановление используемых в среде ОС средств защиты информации). Резервные копии создаются для важных системных каталогов, таких как: /bin, /etc, /var, а также пользовательских данных в каталоге /home.

Перед установкой необходимо провести проверку соответствия контрольных сумм обновлений ОС. Проверка соответствия контрольных сумм обновлений ОС, iso-образов или других файлов, загруженных со сторонних источников, осуществляется с использованием утилиты gostsum из состава ОС.

Пример использования gostsum:

gostsum -d /dev/cdrom

gostsum -d /home/user/test.iso

Обновление безопасности производится согласно разделу «Порядок обновления ОС» документа «Описание применения» с использованием утилиты установки обновлений astra-update для ручной установки обновлений или службы astra-update-service для автоматической.

2.7. Рекомендации по резервному копированию

Перед началом работ по резервному копированию должен быть сформирован и согласован план резервного копирования.

Рекомендуется создание полного образа ОС и установленного ПО. Полный образ представляет собой полную резервную копию всех логических разделов ОС после установки. Образ системы создается для работоспособной операционной системы с установленными приложениями и обновлениями после проведения настройки операционной системы, приложений и средств защиты информации, настройки сетевого окружения для обеспечения работы в сети, а также после создания всех пользовательских и административных учетных записей пользователей. Первичный образ используется для полного восстановления ОС и приложений в случае сбоя или нестабильности работы операционной системы.

В течение эксплуатации операционной системы с периодичностью, установленной в плане резервного копирования, должны создаваться последующие

образы. В каждый момент времени рекомендуется хранить, как минимум, два последних по времени создания образа операционной системы.

Частота архивации пользовательских данных определяется рисками, обусловленными устареванием информации.

Для создания полных резервных копий логических разделов можно использовать утилиту командной строки - dd (dataset definition).

Для создания полных, инкрементных резервных копии пользовательских данных можно использовать утилиту командной строки - rsync.

Для создания полных, дифференциальных, инкрементных копии данных используется программный комплекс Bacula.

Для копирования данных в архив в пределах одного компьютера можно использовать утилиту копирования TAR.

Для восстановления мандатных атрибутов файлов из резервных копий процесс восстановления должен иметь PARSEC-привилегию 0x1000 (PARSEC_CAP_UNSAFE_SETXATTR). Привилегия может быть назначена с использованием инструмента командной строки execaps.

Операции резервного копирования и восстановления подлежат обязательной регистрации в журнале. После завершения каждой операции журнал подлежит проверке.

Создание и восстановление резервных копий осуществляется в соответствии разделом «Резервное копирование и восстановление данных» документа «Руководство администратора. Часть 1» и разделом «Надежное функционирование» документа «Руководство по КСЗ. Часть 1».

Обеспечение отказоустойчивости

В ОС имеется возможность работы на нескольких технических средствах в отказоустойчивом режиме, обеспечивающей доступность сервисов и информации при выходе из строя одного из технических средств. К таким средствам относятся Pacemaker, Corosync, Keepalived, Ceph, HAProxy.

Использование отказоустойчивых решений осуществляется в соответствии с разделом «Средства обеспечения отказоустойчивости и высокой доступности» документа «Руководство администратора. Часть 1».

Обеспечение проверки файловой системы на ошибки

Порядок проверки файловой системы при загрузке с помощью команды fsck задается в конфигурационном файле /etc/fstab в поле <pass>. Для корневой файловой системы следует указывать значение 1, для остальных - 2. Если значение не указано, проверка файловой системы на ошибки и восстановление осуществляться не будут.

3. ПРИМЕНЕНИЕ КОНФИГУРАЦИЙ ПАРАМЕТРОВ БЕЗОПАСНОСТИ

Таблица 3.1 - Применение конфигураций параметров безопасности[1]

№	Наименование настройки	Действия / Параметр	Мера
1.	**Настройка авторизации**		
Настройка параметров политики графического входа			
1.1	Запрет входа в систему без пароля	С целью реализации мер защиты информации, связанных с обязательным прохождением процедур идентификации и аутентификации перед получением доступа к защищаемой информации, требуется обеспечить невозможность входа в систему без пароля. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Дополнительно» → путем выключения опции «Разрешить вход без пароля». - путем редактирования файла /etc/X11/fly-dm/fly-dmrc. Параметру NoPassEnable необходимо присвоить значение false: NoPassEnable=false Пример команды для настройки: sudo sed -Ei 's/NoPassEnable=.*/NoPassEnable=false/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния: cat /etc/X11/fly-dm/fly-dmrc | grep "NoPassEnable" NoPassEnable=false - вход без пароля выключен NoPassEnable=true - вход без пароля включен	ИАФ.1
1.2	Запрет автоматического входа в систему по сохраненным учётным	С целью реализации мер защиты информации, связанных с обязательным прохождением процедур идентификации и аутентификации перед получением доступа к защищаемой информации, требуется обеспечить невозможность автоматического входа в систему по сохраненным учётным данным.	ИАФ.1

[1] В качестве примера приведены меры в соответствии с требованиями, утвержденными приказом ФСТЭК России от 11.02.2013 г. № 17. Конфигурации актуальны и для аналогичных мер защиты информационных систем, обрабатывающих информацию ограниченного доступа.

№	Наименование настройки	Действия / Параметр	Мера
	данным	Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Дополнительно» → путем выключения опции «Разрешить автоматический вход в систему» - с использованием инструмента astra-autologin-control: sudo astra-autologin-control disable Проверка состояния: sudo astra-autologin-control is-enabled enabled - автоматический вход в систему разрешен для определённых пользователей disabled - автоматический вход в систему запрещен	
1.3	Запрет автоматического выбора пользователя для входа	С целью реализации мер защиты информации, связанных с защитой аутентификационной информации от несанкционированного ознакомления и с обязательным прохождением процедур идентификации и аутентификации перед получением доступа к защищаемой информации, требуется обеспечить невозможность автоматического выбора пользователя. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Дополнительно» → путем установки для параметра «Автоматически выбирать пользователя» значения «Нет» и отключения опции «На токене» (при их неиспользовании), позволяющей при подключении токена автоматически выбирать соответствующего пользователя. - путем редактирования файла /etc/X11/fly-dm/fly-dmrc. Для выключения автоматического выбора пользователя для входа параметру PreselectUser необходимо присвоить значение None: PreselectUser=None	ИАФ.1

№	Наименование настройки	Действия / Параметр	Мера
		Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/PreselectUser=.*/PreselectUser=None/g' /etc/X11/fly-dm/fly-dmrc Для отключения выбора соответствующего пользователя при подключении токена необходимо параметру FirstUserToken присвоить значение false: FirstUserToken=false Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/FirstUserToken=.*/FirstUserToken=false/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния: cat /etc/X11/fly-dm/fly-dmrc | grep "FirstUserToken" FirstUserToken=false - выбор соответствующего пользователя при подключении токена отключен FirstUserToken=true - выбор соответствующего пользователя при подключении токена включен cat /etc/X11/fly-dm/fly-dmrc | grep "PreselectUser" PreselectUser=None - автоматический выбор пользователя выключен PreselectUser=Previous - автоматически выбирается пользователь, который входил в систему последним PreselectUser=Default - выбран определенный пользователь	
1.4	Запрет автоматического входа в систему после сбоя X-сервера	С целью реализации мер защиты информации, связанных с обязательным прохождением процедур идентификации и аутентификации перед получением доступа к защищаемой информации, требуется обеспечить невозможность автоматического входа в систему после сбоя. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Дополнительно» → путем отключения опции «Автоматический вход в систему после сбоя X-сервера». - путем редактирования файла /etc/X11/fly-dm/fly-dmrc.	ИАФ.1

№	Наименование настройки	Действия / Параметр	Мера
		Параметру AutoReLogin необходимо присвоить значение false: AutoReLogin=false Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/AutoReLogin=.*/AutoReLogin=false/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния: cat /etc/X11/fly-dm/fly-dmrc | grep "AutoReLogin" AutoReLogin=false - автоматический вход в систему после сбоя X-сервера запрещен AutoReLogin=true - автоматический вход в систему после сбоя X-сервера разрешен	
1.5	Запрет использования удаленных сессий при входе	С целью реализации мер защиты информации, направленных на защиту сетевых соединений, рекомендуется запретить графический вход в систему по сети как в настраиваемый хост, так и из него. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Дополнительно» путем отключения опции «Разрешить удаленные сессии». - путем редактирования файла /etc/X11/fly-dm/Xaccess. Для запрета использования удаленных сессий при входе необходимо, чтобы в файле /etc/X11/fly-dm/Xaccess строки с комментариями #any host can get a login window и #any indirect host can get a chooser начинались с localhost: localhost #any host can get a login window localhost CHOISER BROADCAST #any indirect host can get a chooser Проверка состояния: cat /etc/X11/fly-dm/Xaccess | grep "localhost" Отсутствие вывода команды cat - использование удаленных сессий при входе разрешено Наличие вывода команды cat - использование удаленных	ИАФ.1 УПД.13

№	Наименование настройки	Действия / Параметр	Мера
		сессий при входе запрещено	
1.6	Запрет управления сетевыми подключениям и при входе	С целью реализации мер защиты информации, связанных с обязательным прохождением процедур идентификации и аутентификации перед получением доступа к управлению системой, требуется обеспечить запрет управления сетевыми подключениями пользователями при входе. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Дополнительно» →путем отключения опции «Разрешить управлять доступом к сети». - путем редактирования файла /etc/X11/fly-dm/fly-dmrc. Параметру NetworkAccess необходимо присвоить значение false: NetworkAccess=false Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/NetworkAccess=.*/NetworkAccess=false/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния: cat /etc/X11/fly-dm/fly-dmrc | grep "NetworkAccess" NetworkAccess=false - управление сетевыми подключениями при входе запрещено NetworkAccess=true - управление сетевыми подключениями при входе разрешено	ИАФ.1 УПД.11
1.7	Запрет на ознакомление со списком пользователей на экране входа	С целью реализации мер защиты информации, направленных на защиту аутентификационной информации от несанкционированного ознакомления, требуется обеспечить невозможность ознакомления со списком пользователей системы на экране входа. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» →	ИАФ.1 УПД.11

№	Наименование настройки	Действия / Параметр	Мера
		«Пользователи» путем отключения опции «Показывать список» и опции «Показывать иконки». - путем редактирования файла /etc/X11/fly-dm/fly-dmrc. Параметру UserList необходимо присвоить значение false: UserList=false Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/UserList=.*/UserList=false/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния: cat /etc/X11/fly-dm/fly-dmrc | grep "UserList" UserList=false - ознакомление со списком пользователей на экране входа запрещено UserList=true - ознакомление со списком пользователей на экране входа разрешено	
1.8	Запрет на отображение информации сеанса пользователя на экране блокировки	С целью реализации мер защиты информации, связанных с защитой пользовательских сессий, выполняется настройка запрета отображения информации о сеансе пользователя на устройстве отображения (мониторе) после блокировки сеанса доступа пользователя. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Пользователи» путем включения опции «Скрывать имя (режим блокировщика)». - путем редактирования файла /etc/X11/fly-dm/fly-dmrc. Параметру HideUsername необходимо присвоить значение true: HideUsername=true Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/HideUsername=.*/HideUsername=true/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния:	УПД.10

№	Наименование настройки	Действия / Параметр	Мера
		cat /etc/X11/fly-dm/fly-dmrc | grep "HideUsername" HideUsername=false - отображение информации сеанса пользователя на экране блокировки разрешено HideUsername=true - отображение информации сеанса пользователя на экране блокировки запрещено	
1.9	Запрет на ознакомление с именем хоста на экране входа	С целью реализации мер защиты информации, связанных с обязательным прохождением процедур идентификации и аутентификации перед получением доступа к защищаемой информации, требуется обеспечить невозможность ознакомления с именем хоста на экране входа. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Пользователи» путем включения опции «Скрывать имя хоста». - путем редактирования файла /etc/X11/fly-dm/fly-dmrc. Параметру HideHostName необходимо присвоить значение true: HideHostName=true Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/HideHostName=.*/HideHostName=true/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния: cat /etc/X11/fly-dm/fly-dmrc | grep "HideHostName" HideHostName=false - ознакомление с именем хоста на экране входа разрешено HideHostName=true - ознакомление с именем хоста на экране входа запрещено	
1.10	Запрет автодополнения вводимого имени пользователя	С целью реализации мер защиты информации, направленных на защиту аутентификационной информации от несанкционированного ознакомления, требуется обеспечить невозможность автодополнения имени пользователя. Настройка параметра осуществляется:	ИАФ.11 УПД.11

№	Наименование настройки	Действия / Параметр	Мера
		- с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Пользователи» путем отключения опции «Автодополнение». - путем редактирования файла /etc/X11/fly-dm/fly-dmrc. Параметру UserCompletion необходимо присвоить значение false: UserCompletion=false Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/UserCompletion=.*/UserCompletion=false/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния: cat /etc/X11/fly-dm/fly-dmrc | grep "UserCompletion" UserCompletion=false - автодополнение вводимого имени пользователя запрещено UserCompletion=true - автодополнение вводимого имени пользователя разрешено	
1.11	Запрет графического входа администратора root	Администратор должен получать доступ к системе через учетную запись, входящую в группу astra-admin и имеющую максимальный уровень целостности, а затем использовать sudo для выполнения привилегированных команд. Прямой вход в систему root должен быть разрешен только для использования в экстренных случаях. Настройка параметра осуществляется: - с использованием графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Вход в систему» → «Пользователи» путем отключения опции «Разрешить вход администратору root». - путем редактирования файла /etc/X11/fly-dm/fly-dmrc. Параметру AllowRootLogin необходимо присвоить значение false: AllowRootLogin=false	ИАФ.1 УПД.1

№	Наименование настройки	Действия / Параметр	Мера
		Для установки значения параметра можно воспользоваться командой: sudo sed -Ei 's/AllowRootLogin=.*/AllowRootLogin=false/g' /etc/X11/fly-dm/fly-dmrc Проверка состояния: cat /etc/X11/fly-dm/fly-dmrc | grep "AllowRootLogin" AllowRootLogin=false - графический вход администратора root запрещен AllowRootLogin=true - графический вход администратора root разрешен	
1.12	Настройка входа локальных пользователей в условиях домена	В случае использования в информационной системе доменной структуры следует настроить политику локального входа. Настройка параметра осуществляется: - с использованием графического инструмента «Политика локального входа» (astra-systemsettings astra_kcm_policy_login) по пути: «Пуск» →«Параметры» →раздел «Безопасность» →«Политики учетных записей» → «Политика локального входа». Для доменных компьютеров рекомендуется использовать режим входа «Разрешено администраторам» или «Запрещено всем». При использовании в системе только локальных пользователей должен быть установлен режим «Разрешено всем». - путем редактирования конфигурационного файла /etc/parsec/parsec.conf: • Для разрешения входа для всех локальных учетных записей необходимо параметру login_local установить значение all: login_local all Пример команды для настройки: sudo sed -Ei 's/login_local/#login_local/g' /etc/parsec/parsec.conf sudo echo "login_local all" >> /etc/parsec/parsec.conf • Для разрешения входа только для локальных учетных записей, входящих в локальную группу astra-admin необходимо параметру login_local установить значение admin:	ИАФ.1 УПД.1

№	Наименование настройки	Действия / Параметр	Мера
		login_local admin Пример команды для настройки: sudo sed -Ei 's/login_local/#login_local/g' /etc/parsec/parsec.conf sudo echo "login_local admin" >> /etc/parsec/parsec.conf • Для запрета входа для всех категорий локальных учетных записей необходимо параметру login_local установить значение no: login_local no Пример команды для настройки: sudo sed -Ei 's/login_local/#login_local/g' /etc/parsec/parsec.conf sudo echo "login_local no" >> /etc/parsec/parsec.conf Проверка состояния: cat /etc/parsec/parsec.conf | grep "login_local" login_local all - разрешен вход для всех локальных учетных записей login_local admin - вход разрешен только для локальных учетных записей, входящих в локальную группу astra-admin. login_local no - вход запрещен для всех категорий локальных учетных записей.	
1.13	Удаление пароля root и блокировка входа	Прямой вход в систему root должен быть разрешен только для использования в экстренных случаях. Администратор должен получать доступ к системе через учетную запись, входящую в группу astra-admin и имеющую максимальный уровень целостности, а затем использовать sudo для выполнения привилегированных команд. Настройка осуществляется: - с использованием графического инструмента «Пользователи» (astra-systemsettings astra_kcm_users) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Пользователи и группы» →«Пользователи» →отобразить системных пользователей → выбрать системного пользователя root →нажать на редактирование параметра «Неудачные входы» → активировать опцию «Удаление пароля и блокировка входа».	ИАФ.1 УПД.1

№	Наименование настройки	Действия / Параметр	Мера
		- с использованием консольного инструмента passwd. Для удаления пароля и блокировки пользователя root используется команда: sudo passwd -dl root Проверка состояния: sudo cat /etc/shadow | grep "root" Корректное состояние: root:!:19839:0:99999:7:::	
Настройка параметров политики блокировки учетной записи			
1.14	Количество неуспешных попыток, при превышении которого доступ пользователя в систему будет заблокирован	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка блокировки учетных записей пользователя после установленного количества неудачных попыток вводя пароля. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Блокировка учетной записи» (astra-systemsettings astra_kcm_policy_lockout) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Блокировка» путем установки соответствующего значения для параметра «Неуспешных попыток». Если необходимо использовать индивидуальные настройки для отдельных пользователей, то следует включить опцию «Индивидуальные настройки». Применение индивидуальных настроек для каждого пользователя осуществляется с использованием графического инструмента «Пользователи» (astra-systemsettings astra_kcm_users) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Пользователи и группы» → «Пользователи» → отобразить обычных пользователей → выбрать пользователя → нажать на редактирование параметра «Неудачные входы» → для параметра «максимальное число неудачных входов» устанавливается индивидуальное значение. При этом если в индивидуальных настройках блокировки для параметра установлено значение «0», то максимальное количество неудачных попыток входа будет соответствовать	ИАФ.4 УПД.6

№	Наименование настройки	Действия / Параметр	Мера
		значению, установленному в групповой политике. - путем редактирования конфигурационного файла /etc/pam.d/common-auth. Необходимо в строках, начинающихся с auth requisite pam_faillock.so и auth required pam_faillock.so, присвоить параметру deny соответствующее числовое значение (например, 4). Для установки значения параметра можно воспользоваться командой: sudo sed -i 's/\(deny=\)[^]*/\deny=4/' /etc/pam.d/common-auth и выключить индивидуальные настройки, убрав параметр per_user: sudo sed -i 's/\(per_user\)[^]*/\/' /etc/pam.d/common-auth Проверка состояния: cat /etc/pam.d/common-auth | grep "deny=" cat /etc/pam.d/common-auth | grep "per_user" Для установки индивидуальных настроек количества неуспешных попыток, при превышении которого доступ пользователя в систему будет заблокирован, используется команда: faillog -u <имя_пользователя> -m <необходимое_значение> При этом в /etc/pam.d/common-auth в параметрах pam_faillock.so должен быть установлен параметр per_user. Для установки параметра можно воспользоваться командой: sudo sed -i '/auth.*faillock.so/ s/$/ per_user/' /etc/pam.d/common-auth Для просмотра индивидуальных настроек и фактического количества неуспешных попыток ввода пароля используется инструмент faillog: faillog -u <имя пользователя> Настройка параметра для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути: «Политика» → «Политики паролей» путем выбора	

№	Наименование настройки	Действия / Параметр	Мера
		политики (например, global_policy) и установки значения для параметра «Максимальное количество ошибок» (например, 4). - с использованием инструмента ipa pwpolicy-mod. Например, для изменения параметров глобальной политики global_policy: ipa pwpolicy-mod global_policy --maxfail=4	
1.15	Использование счетчика неудачных попыток для root	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров блокировки учетных записей пользователя после неудачных попыток вводя пароля, в том числе использование счетчика неудачных попыток для учетной записи пользователя root. Настройка параметра осуществляется: - с использованием графического инструмента «Блокировка учетной записи» (astra-systemsettings astra_kcm_policy_lockout) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Блокировка» путем отключения опции «Не использовать счетчик для root». - путем редактирования конфигурационного файла /etc/pam.d/common-auth. Необходимо в конец строк, начинающихся с auth requisite pam_faillock.so и auth required pam_faillock.so, добавить even_deny_root. Пример команды: sudo sed -i '/auth.*faillock.so/ s/$/ even_deny_root/' /etc/pam.d/common-auth Проверка состояния: cat /etc/pam.d/common-auth | grep "even_deny_root" Отсутствие вывода команды cat - использование счетчика неудачных попыток для root выключено Наличие вывода команды cat - использование счетчика неудачных попыток для root включено	ИАФ.4
1.16	Установка периода подсчета неуспешных попыток	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров блокировки учетных записей пользователя после неудачных попыток вводя пароля, в том числе установка периода времени для подсчета неуспешных попыток.	ИАФ.4 УПД.6.

№	Наименование настройки	Действия / Параметр	Мера
		Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Блокировка учетной записи» (astra-systemsettings astra_kcm_policy_lockout) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Блокировка» путем установки значения в секундах для параметра «Период подсчета неуспешных попыток» (например, 900). - путем редактирования конфигурационного файла /etc/pam.d/common-auth. Необходимо в строках, начинающихся с auth requisite pam_faillock.so и auth required pam_faillock.so, присвоить параметру fail_interval числовое значение (например, 900). По умолчанию для модуля pam_faillock.so не задан параметр fail_interval. Для его добавления можно воспользоваться командой: sudo sed -i '/pam_faillock.so/ s/$/ fail_interval=900/' /etc/pam.d/common-auth Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(fail_interval=\)[^]*/fail_interval=900/' /etc/pam.d/common-auth Проверка состояния: cat /etc/pam.d/common-auth | grep "fail_interval" Настройка параметра для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути: «Политика» → «Политики паролей» путем выбора политики (например, global_policy) и установки значения для параметра «Интервал сброса ошибок (в секундах)» (например, 900). - с использованием инструмента ipa pwpolicy-mod. Например, для изменения параметров глобальной политики global_policy используется команда: ipa pwpolicy-mod global_policy --failinterval=900	
1.17	Установка периода разблокировки	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров блокировки учетных записей	ИАФ.4 УПД 6.

№	Наименование настройки	Действия / Параметр	Мера
		пользователя после неудачных попыток вводя пароля, в том числе периода разблокировки. По истечению заданного периода заблокированный пользователь будет разблокирован. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Блокировка учетной записи» (astra-systemsettings astra_kcm_policy_lockout) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Блокировка» путем установки соответствующего значения в секундах для параметра «Период разблокировки» (например, 3600). - путем редактирования конфигурационного файла /etc/pam.d/common-auth. Необходимо в строках, начинающихся с auth requisite pam_faillock.so и auth required pam_faillock.so, присвоить параметру unlock_time числовое значение (например, 3600). По умолчанию для модуля pam_faillock.so не задан параметр unlock_time. Для его добавления можно воспользоваться командой: sudo sed -i '/pam_faillock.so/ s/$/ unlock_time=3600/' /etc/pam.d/common-auth Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(unlock_time=\)[^]*/unlock_time=3600/' /etc/pam.d/common-auth Проверка состояния: cat /etc/pam.d/common-auth | grep "unlock_time" Настройка параметра для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути: «Политика» → «Политики паролей» путем выбора политики (например, global_policy) и установки соответствующего значения для параметра «Длительность блокировки (в секундах)» (например, 3600). - с использованием инструмента ipa pwpolicy-mod. Например, для изменения параметров глобальной политики global_policy:	

№	Наименование настройки	Действия / Параметр	Мера
		ipa pwpolicy-mod global_policy --lockouttime=3600	
1.18	Блокирование учетной записи пользователя за период неактивности	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров блокирования учетной записи пользователя по истечению установленного периода неиспользования. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Блокировка учетной записи» (astra-systemsettings astra_kcm_policy_lockout) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Блокировка» путем установки соответствующего значения периода времени для параметра «Период неактивности» (например, 45 дней). - путем редактирования конфигурационного файла /etc/pam.d/common-auth. Необходимо в строке модуля pam_lastlog.so присвоить параметру inactive соответствующее числовое значение (например, 45 дней). По умолчанию в системе не используется модуль pam_lastlog.so. Его добавление осуществляется с использованием инструмента pam-auth-update (активация модуля «Last login inactivity days»). Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(inactive=\)[^]*/inactive=45/' /etc/pam.d/common-auth Проверка состояния: cat /etc/pam.d/common-auth | grep "inactive"	УПД.1
Настройка параметров политики сложности паролей			
1.19	Проверка наличия имени пользователя в пароле	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе пользователям устанавливается запрет на использование своего имени в качестве пароля. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		«Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» →«Сложность» путем включения опции «Проверка имени пользователя». - путем редактирования конфигурационного файла /etc/pam.d/common-password. Необходимо в строке модуля pam_pwquality.so присвоить параметру usercheck значение 1. По умолчанию для модуля pam_pwquality.so не задан параметр usercheck. Для его добавления можно воспользоваться командой: sudo sed -i '/pam_pwquality.so/ s/$/ usercheck=1/' /etc/pam.d/common-password Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(usercheck=\)[^]*/usercheck=1/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "usercheck" usercheck=1 - проверка наличия имени пользователя в пароле включена usercheck=0 - проверка наличия имени пользователя в пароле выключена	
1.20	Проверка GECOS в пароле	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе включение проверки пароля на предмет содержания в нем каких-либо слов из строк GECOS пользователя. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» →«Сложность» путем включения опции «Проверка GECOS». - путем редактирования конфигурационного файла /etc/pam.d/common-password. Необходимо в строке модуля	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		pam_pwquality.so присвоить параметру gecoscheck значение 1. По умолчанию для модуля pam_pwquality.so не задан параметр gecoscheck. Для его добавления можно воспользоваться командой: sudo sed -i '/pam_pwquality.so/ s/$/ gecoscheck=1/' /etc/pam.d/common-password Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(gecoscheck=\)[^]*/gecoscheck=1/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "gecoscheck" gecoscheck=1 - проверка GECOS в пароле включена gecoscheck=0 - проверка GECOS в пароле выключена	
1.21	Проверка пароля для пользователя root	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе для пользователя root. Настройка параметра осуществляется: - с использованием графического инструмента «Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» →«Сложность» путем включения опции «Применять для пользователя root». - путем редактирования конфигурационного файла /etc/pam.d/common-password. Необходимо в строке модуля pam_pwquality.so добавить enforce_for_root, например, после параметра gecoscheck: sudo sed -i '/gecoscheck=/ s/$/ enforce_for_root/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "enforce_for_root" Отсутствие вывода команды cat - проверка пароля для пользователя root выключена Наличие вывода команды cat - проверка пароля для пользователя root включена	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
1.22	Минимальная длина пароля	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе установка минимальной длины паролей. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Сложность» путем установки соответствующего значения для параметра «Минимальная длина пароля» (например, 8). - путем редактирования конфигурационного файла /etc/pam.d/common-password. Необходимо в строке модуля pam_pwquality.so присвоить параметру minlen соответствующее значение. Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(minlen=\)[^]*/minlen=8/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "minlen" Настройка параметра для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути: «Политика» → «Политики паролей» путем выбора политики (например, global_policy) и установки соответствующего значения для параметра «Минимальная длина» (например, 8). - с использованием инструмента ipa pwpolicy-mod. Например, для изменения параметров глобальной политики global_policy: ipa pwpolicy-mod global_policy --minlength=8	ИАФ.4
1.23	Минимальное количество строчных букв в новом пароле	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе установка минимального количества строчных букв в новом пароле.	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» →«Сложность» путем включения опции «Минимальное количество строчных букв в новом пароле» и установкой соответствующего значения. - путем редактирования конфигурационного файла /etc/pam.d/common-password. В строке модуля pam_pwquality.so необходимо присвоить параметру lcredit соответствующее значение в формате lcredit =-<значение>. По умолчанию для модуля pam_pwquality.so не задан параметр lcredit. Для его добавления можно воспользоваться командой: sudo sed -i '/pam_pwquality.so/ s/$/ lcredit=-1/' /etc/pam.d/common-password Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(lcredit=\)[^]*/lcredit=-2/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "lcredit"	
1.24	Минимальное количество заглавных букв в новом пароле	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе установка минимального количества заглавных букв в новом пароле. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» →«Сложность» путем включения опции «Минимальное количество заглавных букв в новом пароле» и установкой соответствующего значения.	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		- путем редактирования конфигурационного файла /etc/pam.d/common-password. В строке модуля pam_pwquality.so необходимо присвоить параметру ucredit соответствующее значение ucredit =-<значение>. По умолчанию для модуля pam_pwquality.so не задан параметр ucredit. Для его добавления можно воспользоваться командой: sudo sed -i '/pam_pwquality.so/ s/$/ ucredit=-1/' /etc/pam.d/common-password Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(ucredit=\)[^]*/ucredit=-2/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "ucredit"	
1.25	Минимальное количество цифр в новом пароле	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе установка минимального количества цифр в новом пароле. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» →«Сложность» путем включения опции «Минимальное количество цифр в новом пароле» и установкой соответствующего значения. - путем редактирования конфигурационного файла /etc/pam.d/common-password. В строке модуля pam_pwquality.so необходимо присвоить параметру dcredit соответствующее значение в формате dcredit =-<значение>. По умолчанию для модуля pam_pwquality.so не задан параметр dcredit. Для его добавления можно воспользоваться командой: sudo sed -i '/pam_pwquality.so/ s/$/ dcredit=-1/' /etc/pam.d/common-password	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(dcredit=\)[^]*/dcredit=-2/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "dcredit"	
1.26	Минимальное количество «других» символов в новом пароле	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе установка минимального количества «других» символов в новом пароле. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» →«Сложность» путем включения опции «Минимальное количество других символов в новом пароле» и установкой соответствующего значения. - путем редактирования конфигурационного файла /etc/pam.d/common-password. В строке модуля pam_pwquality.so параметру ocredit необходимо присвоить значение в формате ocredit =-<значение>. По умолчанию для модуля pam_pwquality.so не задан параметр ocredit. Для его добавления можно воспользоваться командой: sudo sed -i '/pam_pwquality.so/ s/$/ ocredit=-1/' /etc/pam.d/common-password Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(ocredit=\)[^]*/ocredit=-10/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "ocredit"	ИАФ.4
1.27	Минимальное количество классов символов в	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в том числе установка минимального количества классов	

№	Наименование настройки	Действия / Параметр	Мера
	новом пароле (для доменных пользователей)	символов в новом пароле для доменных пользователей. Настройка сложности пароля для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути: «Политика» → «Политики паролей» путем выбора политики (например, global_policy) и установки значения для параметра «Классы символов». - с использованием инструмента ipa pwpolicy-mod. Например, для изменения параметров глобальной политики global_policy: ipa pwpolicy-mod global_policy --minclass=2	
Настройка параметров политики истории паролей			
1.28	Минимальное количество символов из последнего использованного пароля при создании нового	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики истории паролей, в том числе установка минимального количества символов в новом пароле, которое не должно присутствовать в старом пароле. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Сложность пароля» (astra-systemsettings astra_kcm_policy_complexity) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» →«Сложность» путем включения опции «Минимальное количество измененных символов в новом пароле» и установкой значения (например, 3). - путем редактирования конфигурационного файла /etc/pam.d/common-password. В строке «password requisite pam_pwquality.so» необходимо установить значение для параметра «difok», например, 3. Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(difok=\)[^]*/difok=3/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "difok"	ИАФ.4
1.29	Запрет на	С целью реализации мер защиты информации,	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
	использование пользователями определенного числа последних использованных паролей (в том числе для root)	направленных на защиту учетных записей, выполняется настройка параметров политики истории паролей, в том числе запрет на повторное использование пользователями последних использованных паролей. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «История паролей» (astra-systemsettings astra_kcm_policy_history) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Политики учетных записей» → «История» путем включения опций: «Поддержка истории паролей», «Применять для root», «Количество паролей, которые нужно запомнить» и установки значения (например, 5); - путем задания соответствующей конфигурации в файле /etc/pam.d/common-password. В строку модуля pam_pwhistory.so необходимо добавить параметр «remember» и установить для него соответствующее значение: password requisite pam_pwhistory.so use_authtok enforce_for_root remember=5 По умолчанию в системе не используется модуль pam_pwhistory.so. Для его активации (при отсутствия графики) необходимо создать файл /usr/share/pam-configs/pwhistory и наполнить его содержимым: touch /usr/share/pam-configs/pwhistory echo "Name: Checking password history using pam_pwhistory module Default: none Priority: 1024 Conflicts: unix-zany Password-Type: Primary Password: requisite pam_pwhistory.so use_authtok enforce_for_root remember=5 Password-Initial: requisite pam_pwhistory.so enforce_for_root remember=5 " > /usr/share/pam-configs/pwhistory Внести изменения в /etc/pam.d/common-password:	

№	Наименование настройки	Действия / Параметр	Мера
		sudo sed -i '/password.*requisite.*pam_pwquality.so/a\password requisite pam_pwhistory.so use_authtok enforce_for_root remember=5' /etc/pam.d/common-password Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(remember=\)[^]*/remember=4/' /etc/pam.d/common-password Проверка состояния: cat /etc/pam.d/common-password | grep "remember" Настройка политики истории паролей для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути: «Политика» → «Политики паролей» путем выбора политики (например, global_policy) и установки значения для параметра «Размер журнала (количество паролей)» (например, 5). - с использованием инструмента ipa pwpolicy-mod. Например, для изменения параметров глобальной политики global_policy: ipa pwpolicy-mod global_policy --history=5	
Настройка параметров политики срока действия паролей			
1.30	Минимальное количество дней между сменами пароля	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики срока действия паролей, в том числе установка минимального количества дней между сменами пароля. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Срок действия пароля» (astra-systemsettings astra_kcm_policy_expiration) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Срок действия» путем включения опции «Минимальное количество дней между сменами пароля» и установкой значения (например, 7). - путем редактирования файла /etc/login.defs. Параметру	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		PASS_MIN_DAYS необходимо присвоить значение (например, 7): PASS_MIN_DAYS 7 Для установки значения параметра можно воспользоваться командой: sudo sed -i 's/\(PASS_MIN_DAYS\)[^]*/PASS_MIN_DAYS 7/' /etc/login.defs Проверка состояния: cat /etc/login.defs | grep "PASS_MIN_DAYS" Настройка параметра для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути: «Политика» → «Политики паролей» путем выбора политики (например, global_policy) и установки значения для параметра «Минимальный срок действия (в часах)». - с использованием инструмента ipa pwpolicy-mod. Например, для изменения параметров глобальной политики global_policy: ipa pwpolicy-mod global_policy --minlife=7	
1.31	Максимальное количество дней между сменами пароля	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики срока действия паролей, в том числе установка максимального количества дней между сменами пароля. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Срок действия пароля» (astra-systemsettings astra_kcm_policy_expiration) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Срок действия» путем включения опции «Максимальное количество дней между сменами пароля» и установки значения (например, 60). - путем редактирования файла /etc/login.defs. Параметру PASS_MAX_DAYS необходимо присвоить значение (например, 60): PASS_MAX_DAYS 60 Для изменения значения можно воспользоваться	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		командой: sudo sed -i 's/\(PASS_MAX_DAYS\)[^]*/PASS_MAX_DAYS 60/' /etc/login.defs Проверка состояния: cat /etc/login.defs | grep "PASS_MAX_DAYS" Настройка параметра для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути: «Политика» → «Политики паролей» путем выбора политики (например, global_policy) и установки значения для параметра «Максимальный срок действия (в днях)» (например, 60). - с использованием инструмента ipa pwpolicy-mod. Например, для изменения параметров глобальной политики global_policy: ipa pwpolicy-mod global_policy --maxlife=60	
1.32	Число дней выдачи предупреждения до смены пароля	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики срока действия паролей, в том числе установка числа дней выдачи предупреждения до смены пароля. Настройка параметра для локальных пользователей осуществляется: - с использованием графического инструмента «Срок действия пароля» (astra-systemsettings astra_kcm_policy_expiration) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Срок действия» путем включения опции «Число дней выдачи предупреждения до смены пароля» и установки значения (например, 7). - путем редактирования файла /etc/login.defs. Параметру PASS_WARN_AGE необходимо присвоить значение (например, 7): PASS_WARN_AGE 7 Для установки значения параметра можно воспользоваться командой: sudo sed -i 's/\(PASS_WARN_AGE\)[^]*/PASS_WARN_AGE 7/' /etc/login.defs	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		Проверка состояния: cat /etc/login.defs | grep "PASS_WARN_AGE"	
1.33	Число дней неактивности после устаревания пароля до блокировки учетной записи	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики срока действия паролей, в том числе установка числа дней неактивности после устаревания пароля до блокировки учетной записи. Настройка параметра осуществляется: - с использованием графического инструмента «Срок действия пароля» (astra-systemsettings astra_kcm_policy_expiration) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политики учетных записей» → «Срок действия» путем включения опции «Число дней неактивности после устаревания пароля до блокировки учетной записи» и установки значения (например, 7). - путем редактирования файла /etc/default/useradd. Параметру INACTIVE необходимо присвоить значение (например, 7): INACTIVE=7 По умолчанию в системе не используется параметр INACTIVE. Для его добавления можно воспользоваться командой: echo 'INACTIVE=7' >> /etc/default/useradd Для изменения значения параметра можно воспользоваться командой: sudo sed -i 's/\(INACTIVE=\)[^]*/INACTIVE=11/' /etc/default/useradd	ИАФ.4
Настройка режима запроса пароля при выполнении команды sudo			
1.34	Запрос пароля при выполнении команды sudo	С целью реализации мер защиты информации, направленных на защиту учетных записей, рекомендуется включить режим установки запроса пароля при выполнении команды sudo. Настройка параметра осуществляется: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения	ИАФ.1

№	Наименование настройки	Действия / Параметр	Мера
		программной среды» → «Системные параметры» путем включения опции «Включить ввод пароля для sudo». - с использованием инструмента командной строки astra-sudo-control: sudo astra-sudo-control enable Проверка состояния: sudo astra-sudo-control is-enabled enabled включен disabled выключен	
2	**Настройка учетных записей и управление доступом**		
Настройки параметров политики срока действия учетных записей пользователей			
2.1	Настройка срока действия учетных записей пользователей	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка автоматического блокирования временных учетных записей пользователей по окончании установленного периода времени для их использования. Настройка срока действия для временных учетных записей осуществляется: - с использованием графического инструмента «Пользователи» (astra-systemsettings astra_kcm_users) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Пользователи и группы» →«Пользователи» →отобразить обычных пользователей →выбрать пользователя →нажать на редактирование параметра «Срок действия» → путем включения опции «Срок действия учетной записи пользователя» и установкой даты для каждого временного пользователя. - с использованием инструмента командной строки usermod для каждого временного пользователя: usermod -e YYYY-MM-DD <имя_пользователя>	УПД.1
Ограничение числа параллельных сеансов			
2.2	Ограничение числа параллельных сеансов доступа для учетных записей	С целью реализации мер защиты информации, связанных с ограничением числа параллельных сеансов доступа, выполняется настройка запрета вторичного входа в систему для пользователей или групп. Настройка выполняется в конфигурационном файле /etc/security/limits.conf. Для запрета вторичного входа в	УПД.9

№	Наименование настройки	Действия / Параметр	Мера
	пользователя операционной системы	систему для всех локальных пользователей в конце файла следует добавить запись: * hard maxlogins 1 Пример: echo " * hard maxlogins 1" >> /etc/security/limits.conf Чтобы ограничить вход пользователям по принадлежности к группе (на примере группы test), запись должна иметь следующий вид: %test hard maxlogins 1 Пример команды для настройки: echo "%test hard maxlogins 1" >> /etc/security/limits.conf	
2.3	Ограничение числа параллельных сеансов доступа для учетных записей администраторов операционной системы	С целью реализации мер защиты информации, связанных с ограничением числа параллельных сеансов доступа администраторов, выполняется настройка запрета вторичного входа в систему для администраторов. Настройка выполняется в конфигурационном файле /etc/security/limits.conf. Для запрета вторичного входа в систему для группы администраторов запись должна иметь следующий вид: %astra-admin hard maxlogins 2 Пример команды для настройки: echo "%astra-admin hard maxlogins 2" >> /etc/security/limits.conf	
Настройка параметров блокирования сеанса доступа после времени бездействия			
2.4	Блокирование сеанса доступа пользователя после установленного времени бездействия (неактивности) пользователя	С целью реализации мер защиты информации, связанных с защитой пользовательских сессий, выполняется настройка параметров блокирования сеанса доступа пользователя после установленного времени бездействия (неактивности) пользователя. Настройка глобальной политики для всех пользователей системы осуществляется путем редактирования файла /usr/share/fly-wm/theme.master/themerc. Для параметра ScreenSaverDelay устанавливается количество секунд бездействия (неактивности) пользователя, после которого осуществляется блокирование сеанса доступа пользователя, а также активируются опции других условий блокировки: «При погашенном мониторе» (LockerOnDPMS), «При переходе в режим сна»	УПД.10

№	Наименование настройки	Действия / Параметр	Мера
		(LockerOnSleep), «При переключении на другую сессию» (LockerOnSwitch), «При закрытии крышки ноутбука» (LockerOnLid). Пример конфигурации: [Variables] ScreenSaver="internal fly-modern-locker" ScreenSaverDelay=300 LockerOnDPMS=true LockerOnLid=true LockerOnSleep=true LockerOnSwitch=true Для консольного входа: - в файле /etc/bash.bashrc следует дописать в конец файла: declare -r TMOUT=300 export TMOUT	
2.5	Установка значения времени задержки между попытками ввода пароля	С целью реализации мер защиты информации, связанных с защитой пользовательских сессий, выполняется установка значения времени ожидания перед повторным вводом пароля и настройка уровня звукового сигнала. Настройка глобальной политики для всех пользователей системы осуществляется путем редактирования файла /usr/share/fly-wm/theme.master/themerc. Задается значение для параметров «LockerWrongPasswdTimeout» и «LockerBellLevel», например: LockerWrongPasswdTimeout=2 LockerBellLevel=60	УПД.10
2.6	Ограничение действий пользователей после блокировки	С целью реализации мер защиты информации, связанных с защитой пользовательских сессий, выполняется ограничение действий пользователей по переходу на другую консоль и подключению программ из сети. Настройка глобальной политики для всех пользователей системы осуществляется путем редактирования файла /usr/share/fly-wm/theme.master/themerc. Задается значение true для параметров «LockerTTYLock» и «LockerXaccessLock»: LockerTTYLock=true LockerXaccessLock=true	УПД.10 УПД.11

№	Наименование настройки	Действия / Параметр	Мера
Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации			
2.7	Запрет вывода меню загрузчика	С целью реализации мер защиты информации, связанных с ограничением действий пользователей до прохождения процедур идентификации и аутентификации, рекомендуется установить запрет отображения меню загрузчика. Настройка параметра осуществляется: - с использованием инструмента astra-nobootmenu-control: sudo astra-nobootmenu-control enable Проверка состояния: sudo astra-nobootmenu-control is-enabled enabled - контроль включен disabled - контроль выключен	УПД.11 ОПС.1 УПД.17
2.8	Запрет загрузки в режиме восстановления	С целью реализации мер защиты информации, связанных с ограничением действий пользователей до прохождения процедур идентификации и аутентификации, рекомендуется установить запрет загрузки в режиме восстановления. Настройка параметра осуществляется в конфигурационном файле /etc/default/grub путем добавления параметра GRUB_DISABLE_RECOVERY в значении "true": GRUB_DISABLE_RECOVERY="true" Для применения изменений необходимо обновить загрузчик командой: sudo update-grub	УПД.11 ОПС.1
2.9	Управление блокировкой выключения/ перезагрузки ПК для пользователей	С целью реализации мер защиты информации, связанных с ограничением действий пользователей до прохождения процедур идентификации и аутентификации, рекомендуется установить запрет выключения/ перезагрузки ПК (как локально, так и удаленно) для пользователей. Настройка осуществляется по решению администратора: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения	УПД.11

№	Наименование настройки	Действия / Параметр	Мера
		программной среды» → «Системные параметры» путем включения/отключения опции «Блокировка выключения/перезагрузки ПК для пользователей» - с использованием инструмента командной строки astra-shutdown-lock: sudo astra-shutdown-lock enable/disable Проверка состояния: sudo astra-shutdown-lock is-enabled enabled включен disabled выключен Failed to get unit file state ... сервис не активирован Режим блокирует выключение компьютера пользователями, не являющимися суперпользователями. Для этого права доступа на исполняемый файл /bin/systemctl меняются на 750 (rwx - - - - - -) и меняются параметры в fly-dmrc, после чего команды systemctl могут выполняться только от имени суперпользователя. Изменение режима блокировки вступает в действие немедленно.	
Настройка дискреционных правил разграничения доступом			
2.10	Контроль дискреционных прав доступа к объектам файловой системы	С целью реализации мер защиты информации, направленных на защиту от несанкционированной подмены атрибутов безопасности, а также несанкционированного изменения файлов важных системных директорий, рекомендуется осуществлять периодических контроль установленных правил разграничения доступа. Права доступа для системных файлов должны быть установлены согласно значениям, установленным в базовых конфигурациях, разработанных для ИС. Администратору рекомендуется провести предварительное тестирование используемого системного и прикладного ПО с целью проверки его работоспособности в условиях разработанных конфигураций правил разграничения доступа. Рекомендуется осуществлять контроль атрибутов следующих объектов файловой системы: 1) Необходимо выполнить проверку атрибутов доступа файлов, содержащих информацию о локальных учётных записях. Рекомендуемая конфигурация:	УПД.2

№	Наименование настройки	Действия / Параметр	Мера
		<table><tr><td>/etc/shadow</td><td>-rw-r----- (640) Владелец: root Группа: shadow</td></tr><tr><td>/etc/passwd</td><td>-rw-r--r-- (644) Владелец: root Группа: root</td></tr><tr><td>/etc/group</td><td>-rw-r--r-- (644) Владелец: root Группа: root</td></tr></table> Для просмотра значений атрибутов можно воспользоваться командами: ls -la /etc/shadow ls -la /etc/passwd ls -la /etc/group Для установки корректных прав доступа можно воспользоваться командами: chmod 640 /etc/shadow chown root:shadow /etc/shadow chmod 644 /etc/passwd chown root:root /etc/passwd chmod 644 /etc/group chown root:root /etc/group 2) Выполнить проверку прав доступа разделяемых библиотек и модулей. Файлы из директорий /usr/lib, /usr/lib64, /lib, /lib64 не должны иметь права на запись для группы-владельца и «остальных». Для проверки отсутствия файлов с такими правами доступа можно воспользоваться командами: find /usr/lib /usr/lib64 /lib /lib64 -type f -perm -g=w find /usr/lib /usr/lib64 /lib /lib64 -type f -perm -o=w Для установки корректных прав доступа можно воспользоваться командой: find /usr/lib /usr/lib64 /lib /lib64 -type f -print0 | xargs -0 chmod go-w	

<table>
<tr><th>№</th><th>Наименование настройки</th><th>Действия / Параметр</th><th>Мера</th></tr>
<tr><td></td><td></td><td>Файлы из директорий /lib/modules/<версия ядра>/ не должны иметь права на запись для группы-владельца и «остальных».
Для проверки отсутствия файлов с такими правами доступа можно воспользоваться командами:
find /lib/modules/ -type f -perm -g=w
find /lib/modules/ -type f -perm -o=w
Для установки корректных прав доступа можно воспользоваться командой:
find /lib/modules/ -type f -print0 | xargs -0 chmod go-w

3) Выполнить проверку прав доступа системных конфигурационных файлов. Конфигурационные файлы в /etc должны быть недоступны на запись непривилегированным пользователям.
Для просмотра прав системных конфигурационных файлов можно воспользоваться командами:
find /etc -type f -name "*.conf" -print0 | xargs -0 ls -la
Для проверки отсутствия файлов с такими правами доступа можно воспользоваться командами:
find /etc -type f -name "*.conf" -perm -g=w
find /etc -type f -name "*.conf" -perm -o=w

Для установки корректных прав доступа можно воспользоваться командами:
find /etc -type f -name "*.conf" -print0 | xargs -0 chmod go-w
Также дополнительно проверить права доступа к системным конфигурациям profile, fstab, modprobe, rc#.d:
ls -la /etc/profile.d
ls -la /etc/profile
ls -la /etc/fstab.d
ls -la /etc/fstab
ls -la /etc/fstab.pdac
ls -la /etc/modprobe.d
ls -la /etc/rc*
ls -la /etc/bash.bashrc

<table><tr><td>/etc/profile.d/...</td><td>У файлов внутри директории:
-rw-r--r-- (644)
Владелец: root
Группа: root</td></tr></table></td><td></td></tr>
</table>

№	Наименование настройки	Действия / Параметр		Мера
			У директории /etc/profile.d: rwxr-xr-x (755) Владелец: root Группа: root umask = 077	
		/etc/profile	-rw-r--r-- (644) Владелец: root Группа: root	
		/etc/fstab.d	drwxr-xr-x (755) Владелец: root Группа: root	
		/etc/fstab /etc/fstab.pdac	-rw-r--r-- (644) Владелец: root Группа: root	
		/etc/modprobe.d	Права директории: drwxr-xr-x (755) Владелец: root Группа: root Права файлов внутри: -rw-r--r-- (644) Владелец: root Группа: root	
		/etc/rc0.d /etc/rc1.d /etc/rc2.d /etc/rc3.d /etc/rc4.d /etc/rc5.d /etc/rc6.d /etc/rcS.d	drwxr-xr-x (755) Владелец: root Группа: root	
		/etc/bash.bashrc	-rw-r--r-- (644) Владелец: root Группа: root	
		Для установки корректных прав доступа можно воспользоваться командами: chmod go-w /etc/profile chown root:root /etc/profile		

№	Наименование настройки	Действия / Параметр	Мера
		chmod go-w /etc/fstab chown root:root /etc/fstab chmod go-w /etc/fstab.pdac chown root:root /etc/fstab.pdac chmod go-wx /etc/bash.bashrc chown root:root /etc/bash.bashrc find /etc/profile.d -type f -print0 | xargs -0 chmod u-x,g-wx,o-wx find /etc/modprobe.d -type f -print0 | xargs -0 chmod u-x,g-wx,o-wx find /etc/fstab.d -type f -print0 | xargs -0 chmod u-x,g-wx,o-wx chmod go-w /etc/rc0.d /etc/rc1.d /etc/rc2.d /etc/rc3.d /etc/rc4.d /etc/rc5.d /etc/rc6.d /etc/rcS.d chown root:root /etc/rc0.d /etc/rc1.d /etc/rc2.d /etc/rc3.d /etc/rc4.d /etc/rc5.d /etc/rc6.d /etc/rcS.d 4) Выполнить проверку прав доступа к системным файлам cron. Файл /etc/crontab должен быть недоступен на запись и исполнение для группы-владельца и «остальных». Для проверки можно воспользоваться командой: ls -la /etc/crontab Для установки корректных прав доступа можно воспользоваться командами: chmod go-wx /etc/crontab chown root:root /etc/crontab Файлы директории /etc/cron.d/ не должны иметь права на запись и исполнение для группы-владельца и «остальных». Для просмотра прав можно воспользоваться командой: ls -la /etc/cron.d/ Для установки корректных прав доступа можно воспользоваться командами: find /etc/cron.d/ -type f -print0 | xargs -0 chmod go-wx chown -R root:root /etc/cron.d Файлы из директорий /etc/cron.daily/, /etc/cron.hourly/, /etc/cron.weekly/, /etc/cron.monthly/ не должны иметь права на запись для группы-владельца и «остальных».	

<table>
<tr><th>№</th><th>Наименование настройки</th><th>Действия / Параметр</th><th>Мера</th></tr>
<tr><td></td><td></td><td>Для проверки отсутствия файлов с такими правами доступа можно воспользоваться командами:
find /etc/cron.daily /etc/cron.hourly /etc/cron.weekly /etc/cron.monthly -type f -perm -g=w
find /etc/cron.daily /etc/cron.hourly /etc/cron.weekly /etc/cron.monthly -type f -perm -o=w
Для установки корректных прав доступа можно воспользоваться командами:
find /etc/cron.daily /etc/cron.hourly /etc/cron.weekly /etc/cron.monthly -type f -print0 | xargs -0 chmod go-w
chown -R root:root /etc/cron.daily /etc/cron.hourly /etc/cron.weekly /etc/cron.monthly

Должны быть ограничены права доступа для непривилегированных пользователей к crontab-файлам и исполняемым файлам cron.

<table><tr><td>/usr/sbin/cron
/usr/sbin/anacron
(при наличии)</td><td>-rwxr-xr-x (755)
Владелец: root
Группа: root</td></tr><tr><td>/var/spool/cron/</td><td>drwxr-xr-x (755)
Владелец: root
Группа: root</td></tr><tr><td>/var/spool/cron/crontabs</td><td>drwx-wx--T (1731)
Владелец: root
Группа: crontab</td></tr></table>
Для просмотра прав доступа можно воспользоваться командой:
ls -la /var/spool/cron/
ls -la /var/spool/cron/crontabs
ls -la /usr/sbin/cron
ls -la /usr/sbin/anacron

Для ограничения прав доступа можно воспользоваться командой:
chmod go-w /var/spool/cron/
chown root:root /var/spool/cron/
chown root:crontab /var/spool/cron/crontabs
chmod g-r,o-rwx /var/spool/cron/crontabs
chmod +t /var/spool/cron/crontabs</td><td></td></tr>
</table>

<table>
<tr><th>№</th><th>Наименование настройки</th><th>Действия / Параметр</th><th>Мера</th></tr>
<tr><td></td><td></td><td>chmod go-w /usr/sbin/cron
chown root:root /usr/sbin/cron
chmod go-w /usr/sbin/anacron
chown root:root /usr/sbin/anacron

*Пользовательские файлы заданий cron, если такие имеются, как минимум не должны иметь права доступа на запись для «остальных»

5) Выполнить проверку прав доступа к содержимому домашних директорий пользователей:
- файлы настройки оболочки, такие как:
.bashrc, .profile, .bash_profile, .bash_logout;
- файлы истории команд оболочки, такие как: .bash_history, .history, .sh_history
Например, для пользователя root:
<table><tr><td>/root/.profile</td><td>-rw-r--r-- (644)
Владелец: root
Группа: root</td></tr><tr><td>/root/.bashrc</td><td>-rw-r--r-- (644)
Владелец: root
Группа: root</td></tr></table>Для просмотра прав можно воспользоваться командой:
ls -la /root/.profile
ls -la /root/.bashrc
Для установки корректных прав доступа можно воспользоваться командами:
chown root:root /root/.profile /root/.bashrc
chmod go-wx /root/.profile /root/.bashrc

6) Выполнить проверку прав доступа к исполняемым файлам и библиотекам операционной системы. Файлы из директорий /bin, /usr/bin, /usr/local/bin, /sbin, /usr/sbin, /usr/local/sbin не должны иметь права на запись для «остальных».

Для проверки отсутствия файлов с такими правами доступа можно воспользоваться командами:
find /bin /usr/bin /usr/local/bin /sbin /usr/sbin /usr/local/sbin -type f -perm -o=w</td><td></td></tr>
</table>

№	Наименование настройки	Действия / Параметр	Мера
		Для установки корректных прав доступа можно воспользоваться командами: find /bin -type f -print0 | xargs -0 chmod o-w find /usr/bin -type f -print0 | xargs -0 chmod o-w find /usr/local/bin -type f -print0 | xargs -0 chmod o-w find /sbin -type f -print0 | xargs -0 chmod o-w find /usr/sbin -type f -print0 | xargs -0 chmod o-w find /usr/local/sbin -type f -print0 | xargs -0 chmod o-w	
Разграничение доступа к устройствам			
2.11	Включение механизма контроля подключения устройств	С целью реализации мер защиты, связанных с контролем использования в информационной системе мобильных технических средств, выполняется включение механизма контроля подключения устройств. Включение механизма контроля подключения устройств осуществляется командой: pdac-adm state enable Проверка состояния: pdac-adm state	УПД.15 ЗНИ.5 ЗНИ.6 ЗНИ.7 ЗИС.30
2.12.1	Включение режима запрета монтирования носителей непривилегированным пользователям	С целью реализации мер защиты, связанных с контролем использования в информационной системе мобильных технических средств, выполняется настройка запрета монтирования незарегистрированных съемных носителей информации непривилегированным пользователям. Включение режима запрета монтирования носителей непривилегированным пользователем осуществляется с использованием: - графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения опции «Запрет монтирования носителей непривилегированным пользователем» - с использованием инструмента командной строки astra-mount-lock: sudo astra-mount-lock enable	УПД.15 ЗНИ.5 ЗНИ.6 ЗНИ.7 ЗИС.30

№	Наименование настройки	Действия / Параметр	Мера
		Проверка состояния: sudo astra-mount-lock is-enabled enabled включен disabled выключен После включения режима для того, чтобы непривилегированные пользователи системы могли осуществлять полуавтоматическое монтирование носителей информации, необходимо осуществить их обязательную регистрацию в соответствии с положениями раздела «Средства разграничения доступа к подключаемым устройствам» документа «Руководство администратора. Часть 1» или с пунктом «Постановка на учет защищаемых носителей информации» настоящего документа.	
2.12.2	Постановка на учет защищаемых носителей информации	С целью реализации мер защиты, связанных с контролем использования в информационной системе мобильных технических средств, администратором выполняется регистрация съемных носителей информации. Регистрация для локальных пользователей осуществляется с использованием: - графического инструмента astra-systemsettings по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Устройства и правила» выполнением следующих действий: • на рабочей панели нажать на кнопку [Добавить устройство]; • подключить съемный носитель информации; • во вкладке «Свойства» выбрать параметр для обеспечения гарантированной идентификации устройства (минимальным параметром идентификации является ID_SERIAL или ID_SERIAL_SHORT); • в окне «Добавить устройство» нажать «Да»; • на рабочей панели в поле «Наименование» задать наименование правила; • на рабочей панели установить флаг «Включено», если планируется незамедлительно использовать правило для	

№	Наименование настройки	Действия / Параметр	Мера
		ограничения доступа к устройству; • во вкладке «Общие» выбрать владельца-пользователя и владельца-группу и задать права доступа к файлу устройства. В соответствии с заданными правами будет осуществляться монтирование носителей; • во вкладке МРД задать мандатные атрибуты (при этом уровень конфиденциальности накопителя должен быть не ниже уровня конфиденциальности записываемой на него информации); • во вкладке аудит указать параметры регистрации событий, связанных с файлом устройства; • во вкладке «Правила» добавить дополнительные заготовленные правила идентификации (при наличии); • на панели инструментов нажать на кнопку [Применить]. Регистрация для доменных пользователей осуществляется: - с использованием веб-интерфейса FreeIPA по пути «Политика» → «Политики Parsec» → «Учтенные устройства» → <добавить> → путем указания следующих значений параметров идентификации устройства: • «Наименование учтённого устройства» указывается наименование устройства; • «Владелец устройства» - указывается пользователь-владелец учтенного устройства; • «Группа устройства» — указывается группа-владелец учтенного устройства; • «Атрибуты устройства» - указывается строка ENV{ID_SERIAL}==”…” с указанием атрибута устройства для обеспечения гарантированной идентификации устройства. Пример записи: ENV{ID_SERIAL}==”JetFlash_Transcend_4GB_3KTWWNNM-0:0” Пример команды, позволяющей получить информацию об идентификационном параметре	

№	Наименование настройки	Действия / Параметр	Мера
		устройства: udevadm info /dev/sdb1 | grep ID_SERIAL • «Правила учёта включены» - включение правила учёта устройств. После регистрации устройству во вкладке «Параметры» назначаются права доступа к устройству (параметр «Права доступа к устройству») и мандатные атрибуты безопасности (параметр «Уровень конфиденциальности устройства»). - инструмента ipa parsecdevice-add. Например, для регистрации устройства test для пользователя admin: ipa parsecdevice-add test --device-owner=admin --device-group=admin --device-attr=ENV{ID_SERIAL}==”JetFlash_Transcend_4GB_3KTWWNNM-0:0” --device-status=true.	
2.13	Включение режима запрета форматирования съемных машинных носителей информации непривилегированным пользователям	С целью реализации мер защиты, связанных с контролем доступа к мобильным техническим средствам, выполняется настройка запрета форматирования съемных машинных носителей информации непривилегированным пользователям. Инструмент astra-format-lock устанавливает или отменяет необходимость запроса пароля администратора при форматировании съемных носителей информации. Включение режима запрета форматирования съемных машинных носителей информации непривилегированным пользователям осуществляется: - с использованием инструмента командной строки astra-format-lock: sudo astra-format-lock enable Проверка состояния: sudo astra-format-lock is-enabled enabled включен disabled выключен	УПД.15 ЗНИ.8 ЗИС.30
Ограничение на использование технологий беспроводного доступа			
2.14	Ограничение доступа к подключению к Wi-Fi	С целью реализации мер защиты, связанных с ограничением доступа к беспроводным соединениям, при отсутствии необходимости их использования пользователями, выполняется настройка ограничения доступа к возможности подключения к беспроводным соединениям.	УПД.14 ЗИС.20

№	Наименование настройки	Действия / Параметр	Мера
		Ограничение доступа к подключению к Wi-Fi реализуется с использованием политик PolicyKit. В примере рассмотрено ограничение возможности выполнения подключения к Wi-Fi для всех пользователей, кроме администратора. Ограничение доступа непривилегированным пользователям к возможности управления беспроводными соединениями осуществляется: - с использованием в графической утилиты «Санкции PolicyKit-1» (fly-admin-policykit-1) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Управление доступом» → «Санкции PolicyKit-1» → org.freedesktop → NetworkManager → settings → «Enable or disable Wi-Fi devices» установить следующие значения в панели «Неявные авторизации»: – Удаленная сессия - Запретить – Неактивная консоль - Запретить – Активная консоль - Аутентификация администратора 2) от лица администратора выключить Wi-Fi модуль с помощью команды: nmcli radio wifi off - путем редактирования файла /usr/share/polkit-1/actions/org.freedesktop.NetworkManager.policy. В разделе <action id="org.freedesktop.NetworkManager.enable-disable-wifi"> необходимо установить значение no в строках, соответствующих удаленным сессиям и неактивной консоли, и auth_admin в строке, соответствующей активной консоли: <defaults> <allow_inactive>no</allow_inactive> <allow_active>auth_admin</allow_active> <allow_any>no</allow_any> </defaults> После выполнения перезагрузки, доступ к возможности подключения (и отключения) wifi будет только у администратора. Для редактирования файлов политик можно использовать инструмент mcedit: sudo mcedit /usr/share/polkit-	

№	Наименование настройки	Действия / Параметр	Мера
		1/actions/org.freedesktop.NetworkManager.policy	
2.15	Ограничение доступа к Bluetooth	С целью реализации мер защиты, связанных с ограничением доступа к беспроводным соединениям, выполняется настройка ограничения доступа к Bluetooth. Доступ к устройствам Bluetooth должен предоставляться только для тех пользователей, кому он необходим для выполнения должностных обязанностей. Ограничение доступа к устройствам Bluetooth выполняется путем редактирования настроек файла /etc/dbus-1/system.d/bluetooth.conf. В нем необходимо удалить строки: <policy context="default"> <allow send_destination="org.bluez"/> </policy> Пример команды для настройки: sudo sed -i '/ <policy context="default">/,+2d' /etc/dbus-1/system.d/bluetooth.conf После выполнения перезагрузки, доступ к устройствам bluetooth и утилите "Bluetooth менеджер" будут иметь только пользователи системной группы bluetooth.	УПД.14 ЗИС.20
МКЦ			
2.16	Включение мандатного контроля целостности	В целях реализации мер защиты информации, направленных на защиту параметров настройки средств защиты информации и системного программного обеспечения от несанкционированного изменения, на исключение скрытых каналов (информационных потоков) при защите от угрозы целостности информации, на ограничение запуска компонентов программного обеспечения от имени администраторов безопасности, рекомендуется применение мандатного контроля целостности, который в условиях установленных в компьютерной системе уровней целостности (уровней доверия) обеспечивает невозможность записи отправителем с низким уровнем доверия информации в объекты с более высоким уровнем доверия. Включение мандатного контроля целостности осуществляется:	УПД.5 ОПС.1 ОЦЛ.6 ОЦЛ.8 ЗИС.15 ЗИС.16

№	Наименование настройки	Действия / Параметр	Мера
		- с использованием графического инструмента «Мандатный контроль целостности» (astra-systemsettings astra_kcm_mic) по пути: «Пуск» →«Параметры» →раздел «Безопасность» →«Управление доступом» →«Мандатный контроль целостности» путем включения опции «Подсистема Мандатного Контроля Целостности» и «Защита файловой системы». - с использованием инструмента astra-mic-control: sudo astra-mic-control enable Проверка состояния: sudo astra-mic-control status Назначение мандатных атрибутов целостности локальным пользователям осуществляется с использованием: - графического инструмента «Пользователи» (astra-systemsettings astra_kcm_users) по пути: «Пуск» → «Параметры» →раздел «Безопасность» →«Пользователи и группы» → «Пользователи» → отобразить обычных пользователей → выбрать пользователя → «Уровень целостности» путем определения и установки возможных уровней целостности пользователя. Максимальный уровень целостности присваивается только административным учетным записям пользователей. Назначение мандатных атрибутов целостности для доменных пользователей осуществляется с использованием: - веб-интерфейса FreeIPA по пути: «Идентификация» → «Пользователи» →<пользователь> →«Параметры» путем установки доступного уровня целостности пользователя для параметра «Название уровня целостности». - инструмента ipa user-mod. Например, для изменения уровня целостности пользователя test: ipa user-mod test --miclevel=0 Отключение МКЦ крайне не рекомендуется, так как он обеспечивает защиту критически важных системных файлов и параметров настройки средств защиты информации от несанкционированных изменений в случае эксплуатации дефектов/уязвимостей в программном	

№	Наименование настройки	Действия / Параметр	Мера
		обеспечении информационной системы.	
2.17	Управление запуском сетевых сервисов на пониженном уровне МКЦ	С целью реализации мер защиты информации, направленных на защиту системного программного обеспечения, возможно включение режима запуска сетевых сервисов на пониженном уровне МКЦ. Инструмент astra-ilev1-control при его включении переводит сетевые сервисы apache2, dovecot и exim4 с высокого уровня целостности на первый уровень целостности, для чего в каталоге /etc/systemd размещаются override-файлы для соответствующих сервисов. Включение режима осуществляется с использованием: - графического инструмента «Мандатный контроль целостности» (astra-systemsettings astra_kcm_mic) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Управление доступом» → «Мандатный контроль целостности» путем включения опции «Запуск сервисов на изолированном уровне»; - инструмента командной строки astra-ilev1-control: sudo astra-ilev1-control enable/disable Проверка состояния: sudo astra-ilev1-control is-enabled enabled включен disabled выключен	ЗИС.16 ЗИС.15 ОЦЛ.8 УПД.5 ОПС.1
2.18	Управление запуском контейнеров Docker на пониженном уровне МКЦ	С целью реализации мер защиты информации, направленных на защиту системного программного обеспечения ОС и защищаемых ресурсов от возможного воздействия недоверенного программного обеспечения, исполняемого внутри контейнера, рекомендуется включение режима запуска контейнеров Docker на пониженном уровне МКЦ. Инструмент astra-docker-isolation применяется для перевода службы Docker с высокого уровня целостности на второй уровень целостности, для чего в каталоге /etc/systemd размещается override-файл для службы Docker. Если служба docker не установлена, включение или отключение изоляции docker недоступно. Включение режима осуществляется с использованием инструмента командной строки astra-docker-isolation:	ЗИС.16 ЗИС.15 ОЦЛ.8 УПД.5 ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		sudo astra-docker-isolation enable Проверка состояния: sudo astra-docker-isolation is-enabled enabled включен disabled выключен	
2.19	Управление расширенным режимом мандатного контроля целостности	Расширенный режим МКЦ предназначен для усиления защиты ОС, и включается по решению администратора. При включенном МКЦ (без расширенного режима МКЦ) процесс при его непосредственном запуске наследует метку целостности процесса-родителя (процесс наследует метку целостности запустившего его пользователя). В расширенном режиме МКЦ (strict mode) непосредственный запуск процесса запрещен в том случае, если исполняемый файл, из которого запускается процесс, имеет метку целостности меньше или несравнимую с меткой целостности процесса-родителя. В этом случае процесс возможно запустить только с использованием команды sumic. Включение расширенного режима МКЦ необратимо, после включения он не может быть выключен. Перед включением расширенного режима МКЦ в ОС администратору необходимо провести тестирование используемого прикладного ПО с целью проверки его работоспособности при включенном расширенном режиме МКЦ и определения необходимости его дополнительной настройки. Включение расширенного режима МКЦ осуществляется по решению администратора безопасности путем выполнения от имени администратора команды: sudo astra-strictmode-control enable Выключение расширенного режима мандатного контроля целостности (опция disable) не поддерживается. Изменение режима вступает в действие после перезагрузки.	ЗИС.16 ЗИС.15 ОЦЛ.8 УПД.5 ОПС.1
МРД			
2.20	Включение мандатного управления	По решению администратора об использовании в системе в качестве дополнительной меры защиты информации (например, если в системе хранится и обрабатывается	УПД.12 ЗИС.16 ОЦЛ.6

№	Наименование настройки	Действия / Параметр	Мера
	доступом	информация разного уровня конфиденциальности) - мандатного метода управления доступом, выполняется его включение и настройка. Включение в системе мандатного управления доступом осуществляется с использованием: - графического инструмента «Мандатное управление доступом» (astra-systemsettings astra_kcm_mac) по пути: «Пуск» → «Параметры» → раздел **«**Безопасность**»** → «Управление доступом» → «Мандатное управление доступом» путем включения опции «Подсистема мандатного управления доступом»; - инструмента командной строки astra-mac-control: sudo astra-mac-control enable Настройка уровней конфиденциальности и категорий конфиденциальности, доступных в системе для локальных пользователей, осуществляется с использованием: - инструмента «Мандатное управление доступом» (astra-systemsettings astra_kcm_mac) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Управление доступом» → «Мандатное управление доступом» путем определения и установки возможных уровней конфиденциальности и категорий конфиденциальности. Назначение мандатных атрибутов для локальных пользователей осуществляется с использованием: - графического инструмента «Пользователи» (astra-systemsettings astra_kcm_users) по пути: «Пуск» → «Параметры» →раздел «Безопасность» →«Пользователи и группы» → «Пользователи» → отобразить обычных пользователей → выбрать пользователя → «Категории конфиденциальности» / «Уровни конфиденциальности» путем установки минимального и максимального уровня и категорий конфиденциальности пользователя. Настройка уровней и категорий конфиденциальности, доступных в системе для доменных пользователей, осуществляется с использованием: - веб-интерфейса FreeIPA по пути: «Политика» → «Политики Parsec» → «Уровни конфиденциальности» и	УПД.2

№	Наименование настройки	Действия / Параметр	Мера
		«Категории конфиденциальности» путем определения и установки возможных уровней конфиденциальности и категорий конфиденциальности в домене. - инструмента ipa maclevels-add. Например, для добавления нового уровня конфиденциальности: ipa maclevels-add Уровень_5 --maclevel=5 - инструмента macmaxcat-add. Например, для добавления новой категории конфиденциальности: ipa macmaxcat-add Категория_5 --pcategoryid=5 Назначение мандатных атрибутов для доменных пользователей осуществляется с использованием: - веб-интерфейса FreeIPA по пути: «Идентификация» → «Пользователи» →<пользователь> →«Параметры» путем установки минимального и максимального уровня и категорий конфиденциальности пользователя. - инструмента ipa user-mod. Например, для изменения уровней конфиденциальности пользователя test: ipa user-mod test --macmin=0 --macmax=3	
2.21	Включение режимов AstraMode и MacEnable	Для поддержки работы сервиса apache2 и сервера печати CUPS в условиях мандатного разграничения доступа выполняется их дополнительная настройка. Настройка осуществляется с использованием: - графического инструмента «Мандатное управление доступом» (astra-systemsettings astra_kcm_mac) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Управление доступом» → «Мандатное управление доступом» путем включения опции «Apache» и «Cups». - инструмента командной строки astra-mode-apps: sudo astra-mode-apps enable Для применения изменений требуется перезапуск служб.	УПД.12 ЗИС.16 ОЦЛ.6 УПД.2
2.22	Управление блокировкой использования утилиты sumac	С целью реализации мер защиты информации, направленных на защиту конфиденциальной информации от несанкционированного доступа и возможной утечки в условиях работы мандатного разграничения доступом, рекомендуется включение режима блокировки работы утилит sumac и fly-sumac. Если этот режим включен, даже те пользователи, у которых есть привилегия PARSEC_CAP_SUMAC, не смогут использовать команду	УПД.12 ЗИС.16 ОЦЛ.6 УПД.2 УПД.5 ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		sumac. Для этого устанавливаются права доступа 000 на исполняемый файл sumac и библиотеку libsumacrunner.so. Изменение режима блокировки вступает в действие немедленно. Включение режима осуществляется с использованием: - графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения опции «Блокировка одновременной работы с разными уровнями в пределах одной сессии». - инструмента командной строки astra-sumac-lock: sudo astra-sumac-lock enable/disable Проверка состояния: sudo astra-sumac-lock is-enabled enabled включен disabled выключен	
2.23	Управление блокировкой системных команд	При обработке в одной системе информации разных уровней конфиденциальности рекомендовано включение режима блокировки запуска пользователями следующих программ: df; chatt; arp; ip. Программы блокируются для пользователей с помощью выставления на них прав доступа 750 (rwx r-x - - -). Эти программы необходимо блокировать при обработке в одной системе информации разных уровней конфиденциальности, так как с их помощью можно организовать скрытый канал передачи информации между уровнями. Изменение режима блокировки вступает в действие немедленно. Включение режима осуществляется с использованием: - графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» →	ЗИС.16 ОПС.1 УПД.5

№	Наименование настройки	Действия / Параметр	Мера
		«Ограничения программной среды» → «Системные параметры» путем включения/отключения опции «Блокировка системных команд для пользователей»; - инструмента командной строки astra-commands-lock: sudo astra-commands-lock enable/disable Проверка состояния: sudo astra-commands-lock is-enabled enabled включен disabled выключен	
2.24	Поддержка работы СУБД в МРД	При использовании защищенного сервера СУБД в режиме мандатного управления доступом необходимо: - в конфигурационном файле кластера postgresql.conf для параметра enable_bitmapscan установить значение off и для параметра ac_ignore_socket_maclabel установить значение false; - не допускается отключать аутентификацию субъектов доступа установкой в конфигурационном файле кластера pg_hba.conf режима trust (без аутентификации).	
Настройка механизма фильтрации потоков			
2.25	Управление межсетевым экраном ufw	По решению администратора об использовании встроенных механизмов фильтрации сетевых потоков в качестве дополнительной меры по защите информации при ее передаче выполняется включение встроенного межсетевого экрана. Включение межсетевого экрана ufw осуществляется с использованием: - графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения опции «Включение межсетевого экрана»; - с использованием инструмента командной строки astra-ufw-control: sudo astra-ufw-control enable Проверка состояния: sudo astra-ufw-control is-enabled	УПД.3

№	Наименование настройки	Действия / Параметр	Мера
		enabled включен disabled выключен Настройка межсетевого экрана осуществляется с использованием: - графического инструмента «Gufw Firewall» (gufw) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Межсетевой экран» →«Настройка межсетевого экрана» в минимально необходимой конфигурации, необходимой для работы - по умолчанию все запрещено, кроме необходимых исключений. - инструмента управления сетью iptables, позволяющего администратору управлять входящими и исходящими пакетами данных. Пример добавления правила фильтрации: sudo iptables -A INPUT -p udp --dport 5353 -j DROP После добавления правила необходимо удостоверится в том, что изменения будут сохранены после перезагрузки ОС. Подробнее - https://wiki.astralinux.ru/x/fBsmCQ.	
3	**Ограничение программной среды**		
Права на установку программного обеспечения			
3.1	Права на установку ПО	Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора. Ограничение на использование графической утилиты «Менеджер пакетов Synaptic» осуществляется средствами графической утилиты PolicyKit-1 («Пуск» → «Панель Управления» →«Безопасность» →«Санкции PolicyKit-1). В разделах дерева необходимо выбрать com.ubuntu → pkexec →synaptic – в каждой группе явной (при наличии) и неявной авторизации должны быть заданы параметры аутентификации только для администраторов (групп администраторов): «Аутентификация администратора». - путем редактирования файла политики /usr/share/polkit-1/actions/com.ubuntu.pkexec.synaptic.policy. Для ограничения использования графической утилиты «Менеджер пакетов Synaptic» в файле /usr/share/polkit-1/actions/com.ubuntu.pkexec.synaptic.policy должны быть заданы следующие строки:	ОПС.3

№	Наименование настройки	Действия / Параметр	Мера
		<allow_inactive>auth_admin</allow_inactive> <allow_active>auth_admin</allow_active> <allow_any>auth_admin</allow_any> Пример команды для замены: sudo sed -i 's|\(<allow_inactive>.*\)|<allow_inactive>auth_admin</allow_inactive>|' /usr/share/polkit-1/actions/com.ubuntu.pkexec.synaptic.policy sudo sed -i 's|\(<allow_any>.*\)|<allow_any>auth_admin</allow_any>|' /usr/share/polkit-1/actions/com.ubuntu.pkexec.synaptic.policy sudo sed -i 's|\(<allow_active>.*\)|<allow_active>auth_admin</allow_active>|' /usr/share/polkit-1/actions/com.ubuntu.pkexec.synaptic.policy	
Настройка политик astra-safepolicy			
3.2	Включение запрета установки бита исполнения	С целью реализации мер защиты информации, связанных с ограничением программной среды и направленных на предотвращение несанкционированного создания пользователями или непреднамеренного создания администратором исполняемых сценариев для командной оболочки, выполняется включение режима запрета установки бита исполнения. Режим блокирует возможность установки на файлы бита разрешения исполнения (chmod +x), чем не позволяет пользователям привнести в систему посторонний исполняемый код. При включенной в системе данной функции безопасности установка пакетов программ, создающих в ФС файлы с битом исполнения, будет завершаться с ошибкой. Запрет распространяется, в том числе и на пользователей из группы astra-admin, но не распространяется на root. Изменение режима вступает в действие немедленно. Включение режима осуществляется: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения опции «Запрет установки бита исполнения для всех пользователей, включая администратора».	ОПС.1 ОЦЛ.7

№	Наименование настройки	Действия / Параметр	Мера
		- с использованием инструмента командной строки astra-nochmodx-lock: sudo astra-nochmodx-lock enable Проверка состояния: cat /parsecfs/nochmodx 1 включен 0 выключен	
3.3	Включение блокировки макросов	С целью реализации мер защиты информации, связанных с ограничением программной среды и направленных на защиту от угроз маскирования действий вредоносного кода, выполняется включение режима блокировки исполнения макросов в документах libreoffice. Для этого из меню программ libreoffice удаляются соответствующие пункты, а файлы, отвечающие за работу макросов, перемещаются или делаются недоступными пользователю. Блокировка макросов решает две задачи - защищает от выполнения вредоносного кода при открытии документов и не позволяет злонамеренному пользователю исполнять произвольный код через механизм макросов. Изменение режима блокировки вступает в действие немедленно. Включение режима осуществляется: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения/отключения опции «Блокировка макросов». - с использованием инструмента командной строки astra-macros-lock: sudo astra-macros-lock enable/disable Проверка состояния: sudo astra-macros-lock is-enabled enabled включен disabled выключен	ОПС.1
3.4	Включение блокировки	С целью реализации мер защиты информации, связанных с ограничением программной среды и направленных на	ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
	трассировки ptrace для всех пользователей, включая администраторов	защиту от несанкционированного воздействия на запущенные процессы ОС, выполняется включение режима запрета подключения к другим процессам с помощью ptrace путём установки для параметра ядра kernel.yama.ptrace_scope значения 3. Значение устанавливается сразу при включении этой функции и настраивается сохранение этого значения после перезагрузки. Функция не может быть отключена без перезагрузки. Включение режима осуществляется: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения/отключения опции «Блокировка трассировки ptrace для всех пользователей, включая администраторов». - с использованием инструмента командной строки astra-ptrace-lock: sudo astra-ptrace-lock enable/disable Проверка состояния: sudo astra-ptrace-lock is-enabled enabled включен disabled выключен	
3.5	Установка системных ограничений ulimits /etc/security/limits.conf	С целью реализации мер защиты информации, направленных на предотвращение нарушений доступности системы в результате исчерпания ресурсов, настраиваются ограничения на использование пользователями некоторых ресурсов системы. Настройка осуществляется: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения опции «Включение системных ограничений ulimits»;	ЗИС.22 ОДТ.1, ОДТ.3 УПД.9

№	Наименование настройки	Действия / Параметр	Мера
		- с использованием инструмента командной строки astra-ulimits-control: sudo astra-ulimits-control enable/disable Проверка состояния: sudo astra-ulimits-control is-enabled enabled включен disabled выключен	
3.6	Настройка дисковых квот в ОС	С целью реализации мер защиты информации, направленных на предотвращение нарушений доступности системы в результате исчерпания ресурсов, настраиваются ограничения на использование пользователями дисковой памяти и количества файлов, принадлежащих пользователю. Настройка выполняется с использованием: - графического инструмента «Квоты» (astra-systemsettings astra_kcm_quotas) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» →«Квоты» путем: 1) включения опций «Поддержка квот для пользователей» и/или «Поддержка квот для групп» во вкладке «Общие настройки»; 2) настройкой оповещений для пользователей и групп о превышении установленных квот во вкладке «Настройки оповещений»; 3) установкой мягких и жестких ограничений на использование пользователями/группами дисковой памяти и количества файлов во вкладке «Группы» и «Пользователи». - путем редактирования файла /etc/fstab. Для включения/выключения поддержки пользовательских и групповых квот необходимо: 1) Добавить опции usrquota и grpquota в файл /etc/fstab. Опции необходимо добавлять в строку соответствующей файловой системы, для которой необходимо включить поддержку квот. Добавить опции в файл /etc/fstab можно либо с помощью ручного редактирования файла, либо с помощью команды: sed -i '/^<uid строки с необходимым разделом>/	ЗИС.22 ОДТ.1 ОДТ.3

№	Наименование настройки	Действия / Параметр	Мера
		s/defaults/&,usrquota,grpquota/g' /etc/fstab 2) Перезагрузить систему 3) Создать файлы пользовательских и групповых квот с помощью утилиты quotacheck: quotacheck -um <ФС в формате /dev/...> quotacheck -gm <ФС в формате /dev/...> 4) Включить пользовательские и групповые квоты: quotaon -u <ФС в формате /dev/...> - пользовательские квоты quotaon -g <ФС в формате /dev/...> - групповая квота Для отключения пользовательских и групповых квот необходимо использовать команды: quotaoff -u <ФС в формате /dev/...> - пользовательские квоты quotaoff -g <ФС в формате /dev/...> - групповая квота *При использовании утилит quotacheck, quotaon и quotaoff необходимо указывать файловую систему, для которой были добавлены опции usrquota и grpquota в /etc/fstab. Для управления мягкими и жесткими ограничениями для пользователей и групп необходимо использовать утилиту edquota. edquota <имя пользователя>\<наименование группы> При вводе команды открывается редактор, в котором можно задать мягкие и жесткие ограничения для указанного в команде пользователя или группы Настройка оповещений для пользователей и групп о превышении установленных квот выполняется в файле /etc/cron.d/warnquota Для создания оповещения необходимо добавить в файл /etc/cron.d/warnquota строку "3 0 5 * * root warnquota -u -g" echo "3 0 5 * * root warnquota -u -g" >> /etc/cron.d/warnquota	
3.7	Включение блокировки	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на	ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
	автоматического конфигурирования сетевых подключений	ограничение действий пользователей по возможностям управления сетевыми подключениями, выполняется включение режима блокировки автоматического конфигурирования сетевых подключений. В результате включения режима блокируются службы NetworkManager, network-manager и connman, а также отключается элемент управления сетью в трее графического интерфейса. Включение/отключение блокировки автоматического конфигурирования сетевых подключений осуществляется: - с использованием инструмента командной строки astra-noautonet-control: sudo astra-noautonet-control enable Проверка состояния: sudo astra-noautonet-control is-enabled enabled включен disabled выключен	
3.8	Ограничение доступа root по SSH	С целью реализации мер защиты, направленных на ограничение доступа суперпользователя root посредством SSH, выполняется включение режима блокировки доступа по протоколу SSH для учетной записи root. Управление блокировкой в системе выполняется, если в системе установлен пакет ssh. Включение запрета доступа для учетной записи root по протоколу SSH осуществляется: - с использованием инструмента командной строки astra-rootloginssh-control: sudo astra-rootloginssh-control enable Проверка состояния: sudo astra-rootloginssh-control is-enabled enabled включен disabled выключен	ОПС.1
3.9	Включение блокировки клавиши SysRq	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на защиту от несанкционированного воздействия на компоненты ОС, выполняется включение режима блокировки клавиши SysRq. Режим отключает функции системы, доступные при нажатии клавиши SysRq, так как их использование пользователем может быть небезопасно.	ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		Для этого изменяется значение параметра kernel.sysrq. Значение параметра сохраняется в файл /etc/sysctl.d/999-astra.conf. По умолчанию эта функция безопасности включена, т.е. клавиша SysRq не работает. Ограничение работы функций системы, доступных при нажатии клавиши SysRq, осуществляется с использованием: - графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения/отключения опции «Блокировка клавиш SysRq для всех пользователей, включая администраторов»; - с использованием инструмента командной строки astra-sysrq-lock: sudo astra-sysrq-lock enable Проверка состояния: cat /proc/sys/kernel/sysrq 0 включен 1 выключен	
3.10	Управление режимом работы файловой системы ОС - «только чтение»	В тех случаях, когда носитель, на котором расположена корневая ФС, аппаратно защищен от записи либо необходимо программно защитить его от изменений, рекомендовано применение режима работы файловой системы ОС - «только чтение». Инструмент astra-overlay включает overlay на корневой ФС. Фактическое содержимое корневой ФС монтируется в overlay одновременно с файловой системой, хранящейся в памяти. После этого все изменения файлов сохраняются только в памяти, а файловая система, хранящаяся на носителе, остается без изменений. После перезагрузки все изменения теряются, и система каждый раз загружается в исходном состоянии. Функционал overlay не касается файловых систем, хранящихся на отдельных разделах, отличных от	ЗИС.18

№	Наименование настройки	Действия / Параметр	Мера
		корневого. Если, например, /home хранится на отдельном разделе или носителе, вносимые в него изменения будут сохраняться после перезагрузки. Изменение режима работы вступает в действие после перезагрузки. При включении данного режима дисковый раздел, в котором находится корневая файловая система, будет перемонтирован в специальном режиме временной файловой системы, при котором вносимые в файлы изменения будут сохраняться только до перезагрузки. Данный режим позволяет защитить от изменений системные файлы, однако файлы, в которых должны сохраняться постоянные изменения (например, домашние каталоги пользователей) должны находиться в другом дисковом разделе. Включение режима осуществляется по решению администратора: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения/отключения опции «Включить режим работы файловой системы ОС →«только чтение»; - с использованием инструмента командной строки astra-overlay: sudo astra-overlay enable/disable Проверка состояния: sudo astra-overlay is-enabled enabled включен disabled выключен	
3.11	Включение блокировки консоли для пользователей, не входящих в группу astra-console	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на ограничение действий пользователей по возможностям работы в консоли и терминалах, выполняется включение блокировки консоли для пользователей, не входящих в группу astra-console. Инструмент astra-console-lock осуществляет блокировку доступа к консоли и терминалам	ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		для пользователей, не входящих в группу astra-console. Если при включении блокировки группа astra-console отсутствует в ОС, то она будет создана автоматически. При этом в нее будут включены пользователи, состоящие в группе astra-admin на момент включения этой функции. Включение режима блокировки терминала и псевдотерминала tty1-tty6 (Ctrl/Alt/F1...F6) для всех пользователей, не состоящих в группе astra-console, осуществляется: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения/отключения опции «Включить блокировку консоли для пользователей, не входящих в группу astra-console»; - с использованием инструмента командной строки astra-console-lock sudo astra-console-lock enable Проверка состояния: sudo astra-console-lock is-enabled enabled включен disabled выключен	
3.12	Блокировка интерпретаторов	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на ограничение действий пользователей по возможностям интерактивного исполнения команд или программ, написанных на интерпретируемых языках программирования Python, Perl, Expect, Ruby, dash, irb, csh lua, ksh, tcl, tk, zsh, выполняется включение блокировки интерпретаторов (кроме bash). Включение режима блокировки осуществляется: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем	ОПС.1 ОЦЛ.1 ЗИС.7 ЗИС.22

№	Наименование настройки	Действия / Параметр	Мера
		включения опции «Включить блокировку интерпретаторов кроме Bash для пользователей»; - с использованием инструмента командной строки astra-interpreters-lock: sudo astra-interpreters-lock enable Проверка состояния: sudo astra-interpreters-lock is-enabled enabled включен disabled выключен	
3.13	Блокировка интерпретатора Bash	Блокировка интерпретатора Bash аналогична блокировке других интерпретаторов команд, вынесена в отдельную блокировку, так как ее активация может стать причиной некорректной работы служб, в том числе работающих в фоновом режиме. В частности, после блокировки интерпретатора bash становится невозможным вход непривилегированных пользователей, использующих bash в качестве командной оболочки, в консольную сессию. Не распространяет своё действие на пользователей из группы astra-admin. Изменение режима блокировки вступает в действие немедленно. Блокировка включается по решению администратора: - с использованием графического инструмента «Системные параметры» (astra-systemsettings astra_kcm_system_parameters) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системные параметры» путем включения опции «Включить блокировку интерпретатора Bash для пользователей»; - с использованием инструмента командной строки astra-bash-lock: sudo astra-bash-lock enable/disable Проверка состояния: sudo astra-bash-lock is-enabled enabled включен disabled выключен	ОПС.1 ОЦЛ.1 ЗИС.7 ЗИС.22

№	Наименование настройки	Действия / Параметр	Мера
Настройка киоска			
3.14	Применение графического киоска Fly	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на ограничение запуска приложений пользователем, возможно применение графического киоска Fly. При использовании графического киоска пользователю или группе пользователей разрешается запускать только те приложения, которые явно указаны в их профиле. На пользователя действуют ограничения только если подкаталог с его профилем существует в каталоге /etc/fly-kiosk или этот пользователь входит в группу, для которой существует профиль в каталоге /etc/fly-kiosk (этот каталог по умолчанию не существует, и создается при включении режима графического киоска). Профиль пользователя или группы представляет собой набор ярлыков и настроек. Настройка параметров киоска осуществляется: - с использованием графической утилиты «Графический киоск» (astra-systemsettings astra_kcm_graphics_kiosk) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Ограничения программной среды» → «Графический киоск». Переход к настройке графического киоска для каждого пользователя также возможен из графического инструмента «Пользователи» (astra-systemsettings astra_kcm_users) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Пользователи и группы» → «Пользователи» →отобразить обычных пользователей → выбрать пользователя → «Графический киоск». Для пользователя настраивается режим киоска при работе с приложениями из списка. Если в списке одно приложение, то режим киоска включается при работе с этим приложением. Если в списке несколько приложений, то запускается рабочий стол с этими приложениями. Все доступные каталоги, ярлыки и т.д. устанавливаются в соответствии с предоставленным доступом. - путем формирования файлов киоска для пользователя. Пример ручной настройки киоска для пользователя user: 1) В каталоге /etc/fly-kiosk/ необходимо создать директорию с именем, соответствующим пользователю,	ОПС.1 ОЦЛ.6 ЗИС.1

№	Наименование настройки	Действия / Параметр	Мера
		для которого производится настройка графического киоска. Пример: mkdir /etc/fly-kiosk/user 2) Назначить созданной директории корректные права доступа. Пример: chmod 750 /etc/fly-kiosk/user chown root:user /etc/fly-kiosk/user 3) Внутри созданной директории user создать следующие директории: • autostart • desktop • scripts • single • toolbar И следующие файлы: • exit.desktop • fly-kiosk.conf Пример: mkdir /etc/fly-kiosk/user/autostart mkdir /etc/fly-kiosk/user/desktop mkdir /etc/fly-kiosk/user/scripts mkdir /etc/fly-kiosk/user/single mkdir /etc/fly-kiosk/user/toolbar touch /etc/fly-kiosk/user/exit.desktop touch /etc/fly-kiosk/user/fly-kiosk.conf 4) Назначить созданным директориям и файлам корректные права доступа. Пример: chmod 755 /etc/fly-kiosk/user/autostart chmod 755 /etc/fly-kiosk/user/desktop chmod 755 /etc/fly-kiosk/user/scripts chmod 755 /etc/fly-kiosk/user/single chmod 755 /etc/fly-kiosk/user/toolbar chmod 644 /etc/fly-kiosk/user/exit.desktop chmod 644 /etc/fly-kiosk/user/fly-kiosk.conf chown root:user /etc/fly-kiosk/user/autostart chown root:user /etc/fly-kiosk/user/desktop	

№	Наименование настройки	Действия / Параметр	Мера
		chown root:user /etc/fly-kiosk/user/scripts chown root:user /etc/fly-kiosk/user/single chown root:user /etc/fly-kiosk/user/toolbar chown root:user /etc/fly-kiosk/user/exit.desktop 5) В директории /etc/fly-kiosk/user/desktop необходимо создать файлы приложений на рабочем столе с наименованием org.kde.<наименование приложения>.desktop. Пример создания файла для приложения kate /etc/fly-kiosk/user/desktop/org.kde.kate.desktop: touch /etc/fly-kiosk/user/desktop/org.kde.kate.desktop Пример заполнения файла для приложения kate: echo '[Desktop Entry] Name=Kate GenericName=Advanced Text Editor Type=Application Comment=KDE Advanced Text Editor Exec=/usr/bin/kate -b %U Icon=kate Comment[ru]=Улучшенный текстовый редактор от KDE GenericName[ru]=Улучшенный текстовый редактор Name[ru]=Редактор Kate' >> /etc/fly-kiosk/user/desktop/org.kde.kate.desktop Пример назначения прав доступа к файлу для приложения kate: chmod 644 /etc/fly-kiosk/user/desktop/org.kde.kate.desktop 6) В директории /etc/fly-kiosk/user/scripts необходимо создать файл powersave-mode.sh touch /etc/fly-kiosk/user/scripts/powersave-mode.sh Содержимое файла /etc/fly-kiosk/user/scripts/powersave-mode.sh: echo '#!/bin/bash configdir="/home/$USER/.config" config=$configdir/powermanagementprofilesrc function createconfig { touch $config	

№	Наименование настройки	Действия / Параметр	Мера

		cat >> $config << EOF
		[AC][DPMSControl]
		idleTime=0
		
		[AC][DimDisplay]
		idleTime=0
		
		[Battery][DPMSControl]
		idleTime=0
		
		[Battery][DimDisplay]
		idleTime=0
		
		[Battery][SuspendToRam]
		idleTime=0
		
		[LowBattery][DPMSControl]
		idleTime=0
		
		[LowBattery][DimDisplay]
		idleTime=0
		
		[LowBattery][SuspendToRam]
		idleTime=0
		
		EOF
		}
		
		mkdir -p "/home/$USER/.config"
		
		if [! -e $config]; then
		mkdir -p $configdir
		createconfig
		fi
		
		if grep -q "PowerSaveMode=true" $FLY_KIOSK_CONFIG_DIR/fly-kiosk.conf; then
		sed -i "s/idleTime.*/idleTime=600/g" $config
		else
		sed -i "s/idleTime.*/idleTime=0/g" $config
		fi	

№	Наименование настройки	Действия / Параметр	Мера
		sed -i "s/;idleTime/idleTime/g" $config' >> /etc/fly-kiosk/user/scripts/powersave-mode.sh Права доступа к файлу /etc/fly-kiosk/user/scripts/powersave-mode.sh: chmod 755 /etc/fly-kiosk/user/scripts/powersave-mode.sh 7) В директории /etc/fly-kiosk/user/toolbar необходимо создать файл start.desktop touch /etc/fly-kiosk/user/toolbar/start.desktop Содержимое файла /etc/fly-kiosk/user/toolbar/start.desktop: echo '[Desktop Entry] Name=Menu "Start" Type=Application Exec=FLYWM_POPUP_START_MENU Icon=astra-simplified Name[ru]=Меню "Пуск"' >> /etc/fly-kiosk/user/toolbar/start.desktop Права доступа к файлу /etc/fly-kiosk/user/toolbar/start.desktop: chmod 644 /etc/fly-kiosk/user/toolbar/start.desktop 8) Указать в файле /etc/fly-kiosk/user/exit.desktop необходимые параметры, например, с помощью команды echo: echo '[Desktop Entry] Name=Exit... Type=Application Exec=fly-shutdown.sh Icon=system-log-out Name[ru]=Завершение работы...' >> /etc/fly-kiosk/user/exit.desktop 9) Указать в файле /etc/fly-kiosk/user/fly-kiosk.conf необходимые параметры, например, с помощью команды echo: echo '[%General] EditableDesktop=false EditableTheme=false IsGroup=false	

№	Наименование настройки	Действия / Параметр	Мера
		PowerSaveMode=false' >> /etc/fly-kiosk/user/fly-kiosk.conf Выполнение вышеперечисленных пунктов необходимо для базовой настройки графического киоска для пользователя.	
3.15	Применение системного киоска	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на ограничение возможностей, предоставляемых непривилегированным пользователям, рекомендовано применение системного киоска - инструмента подсистемы безопасности PARSEC, обеспечивающего усиленную защиту от запуска неразрешенных программ. В отличие от графического киоска, ограничивающего доступ на уровне графической среды, системный киоск ограничивает пользователя на более низком уровне - уровне ядра системы. Системный киоск обеспечивает более надежную защиту от несанкционированного доступа, чем графический. Настройка и включение режима системного киоска осуществляется в соответствии с положениями документа «Руководство по КСЗ. Часть 1», пункт «Режим Киоск-2». Настройку режима можно осуществить: - с использованием графического инструмента «Системный кисок» (fly-admin-kiosk) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Ограничения программной среды» → «Системный киоск». Инструмент позволяет включать и отключать режим киоска через графическое меню «Файл» → «Включить режим киоска» или кнопкой с изображением ключей в панели кнопок, а также позволяет создавать и изменять профили пользователей. - путем формирования файлов киоска для пользователя. Пример ручной настройки системного киоска для пользователя user: 1) В директории /etc/parsec/kiosk2/ создать файл с именем, соответствующим имени пользователя, для которого настраивается системный киоск touch /etc/parsec/kiosk2/user 2) В файле etc/parsec/kiosk2/user должны содержаться подключенные профили для пользователя (например,	ОПС.1 ОЦЛ.6 ЗИС.1 ЗИС.22

№	Наименование настройки	Действия / Параметр	Мера
		libreoffice) из каталога /etc/parsec/kiosk2/kiosk2-profiles echo '@include libreoffice' >> /etc/parsec/kiosk2/user 3) Установить значение "1" в файле /etc/parsec/kiosk2_enforce	
Настройка ЗПС			
3.16	Включение механизма контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на обеспечение динамического контроля целостности запускаемых компонент программного обеспечения, выполняется включение механизма контроля целостности исполняемых файлов и разделяемых библиотек формата ELF. Перед настройкой следует ознакомиться с положениями документа "Руководство по КСЗ. Часть 1", раздел «Замкнутая программная среда», и изучить программную документацию man bsign и man gpg. Динамический контроль вычисляет и проверяет электронную цифровую подпись исполняемых модулей в момент их запуска. Если цифровой подписи нет или она неправильная, в запуске программ будет отказано. Включение механизма проверки подписей в режиме контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение осуществляется: - с использованием графической утилиты «Замкнутая программная среда» (astra-systemsettings astra_kcm_digsig) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Ограничения программной среды» → «Замкнутая программная среда» путем включения параметра «Контроль исполняемых файлов»; - путем редактирования файла /etc/digsig/digsig_initramfs.conf – для параметра DIGSIG_ELF_MODE установить значение 1: DIGSIG_ELF_MODE=1 После внесения изменений в конфигурационный файл /etc/digsig/digsig_initramfs.conf необходимо выполнить: sudo update-initramfs -u -k all - с использованием инструмента командной строки astra-digsig-control: sudo astra-digsig-control enable Проверка состояния:	ОПС.1 ОЦЛ.1 ИАФ.7 ЗИС.7 ЗИС.15 ЗИС.18 ЗИС.22

№	Наименование настройки	Действия / Параметр	Мера
		sudo astra-digsig-control is-enabled enabled включен disabled выключен	
3.17	Включение механизма контроля целостности файлов при их открытии на основе цифровой подписи в расширенных атрибутах файловой системы	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на обеспечение динамического контроля целостности не подлежащих изменению архивных файлов и параметров настройки программного обеспечения и средств защиты информации, выполняется включение и настройка механизма контроля целостности файлов при их открытии на основе цифровой подписи в расширенных атрибутах файловой системы. В данном режиме при нарушении целостности файлов доступ на чтение к ним будет заблокирован. Для проверки подписи открываемых файлов в расширенных атрибутах используется дополнительный набор (изначально пустой) ключей. Для создания дополнительного ключа и его использования для подписывания объектов необходимо создать ключевую пару и выполнить экспорт созданного ключа в каталог /etc/digsig/xattr_keys/ согласно положениями документа "Руководство по КСЗ. Часть 1", раздел «Подписывание файлов». Для постановки на контроль файлов необходимо настроить шаблоны имен, используемых при проверке цифровой подписи в расширенных атрибутах ФС: - в файле /etc/digsig/xattr_control задать их список. Каждая строка задает свой шаблон в виде маски полного пути. Далее ключом пользователя осуществляется подпись объектов, подлежащих контролю с использованием утилиты bsign. После выполняется включение механизма проверки подписей в режиме запрета открытия поставленных на контроль файлов с неверной цифровой подписью или без цифровой подписи в расширенных атрибутах файловой системы: - с использованием графической утилиты «Замкнутая программная среда» (astra-systemsettings astra_kcm_digsig) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Ограничения программной среды» → «Замкнутая	ОПС.2 АНЗ.3 ОПС.1 ИАФ.7 ЗИС.15

№	Наименование настройки	Действия / Параметр	Мера
		программная среда» путем включения параметра «Контроль расширенных атрибутов». На предложение перезагрузки ответить положительно. - путем редактирования файла /etc/digsig/digsig_initramfs.conf - для значения DIGSIG_XATTR_MODE установить значение 1: DIGSIG_XATTR_MODE=1 После внесения изменений в конфигурационный файл /etc/digsig/digsig_initramfs.conf необходимо выполнить: sudo update-initramfs -u -k all Пример постановки на контроль файла /etc/fstab и включения режима проверки подписи открываемых файлов в расширенных атрибутах: sudo su gpg --full-generate-key gpg --export "TestTest <test@astralinux.ru>" > /etc/digsig/xattr_keys/secondary_gost_key.gpg update-initramfs -u -k all reboot bsign --sign --xattr /etc/fstab sudo getfattr -dm- /etc/fstab sudo echo "/etc/fstab" >> /etc/digsig/xattr_control sudo sed -i 's/DIGSIG_XATTR_MODE=0/DIGSIG_XATTR_MODE=1/g' /etc/digsig/digsig_initramfs.conf sudo update-initramfs -u -k all sudo reboot Внимание: после выполненных действий, при нарушении целостности /etc/fstab доступ на чтение к нему будет заблокирован, что может заблокировать работу ОС.	
4	**Защита памяти**		
4.1	Включение механизма очистки памяти	С целью реализации мер защиты, связанных с очисткой освобождаемой памяти (остаточной информации), и направленных на исключение несанкционированного доступа к защищаемой информации, применяется механизм очистки освобождаемой внешней памяти. Включение механизма обеспечивает очистку неиспользуемых блоков файловой системы непосредственно при их освобождении, а также очистку разделов страничного обмена. Работа данного механизма может снижать скорость выполнения операций удаления и	ЗИС.21 ЗНИ.4 ЗНИ.8 ОПС.4 ЗИС.16

№	Наименование настройки	Действия / Параметр	Мера
		усечения размера файла. Механизм очистки памяти активируется параметром secdelrnd в конфигурационном файле /etc/fstab для раздела файловой системы, на котором требуется очистка блоков памяти при их освобождении (например, /dev/sda1). В список параметров монтирования добавляется параметр secdelrnd. Пример: /dev/sda1 /home ext4 acl,defaults,secdelrnd 0 2 Включение механизма очистки блоков памяти при их освобождении может быть выполнено: - с использованием графической утилиты «Политика очистки памяти» (astra-systemsettings astra_kcm_policy_clean_memory) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политика очистки памяти» →«Гарантированное удаление файлов и папок» путем настройки параметров очистки для установленных разделов. - с использованием инструмента astra-secdel-control. Инструмент astra-secdel-control включает и выключает механизм безопасного удаления файлов на разделах с файловыми системами ext2, ext3, ext4, XFS, указанных в /etc/fstab, в режиме 2х кратной очистки каждого байта в освобождаемой области посредством псевдослучайных сигнатур. Его включение осуществляется командой: sudo astra-secdel-control enable Проверка состояния: sudo astra-secdel-control is-enabled enabled включен disabled выключен Примечание: механизм очистки памяти при применении на SSD-накопителях технически не может гарантировать полное удаление информации, ранее записанной на SSD-накопитель.	
4.2	Включение механизма очистки разделов	С целью реализации мер защиты, связанных очисткой освобождаемой памяти и направленных на исключение несанкционированного доступа к защищаемой информации, применяется механизм очистки разделов	ЗИС.21 ОПС.4 ЗИС.16

№	Наименование настройки	Действия / Параметр	Мера
	подкачки	подкачки. Включение очистки разделов подкачки осуществляется: - с использованием графической утилиты «Политика очистки памяти» (astra-systemsettings astra_kcm_policy_clean_memory) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Политика очистки памяти» →«Гарантированное удаление файлов и папок» путем включения опции «Очистка разделов подкачки». - с использованием консольной утилиты astra-swapwiper-control: sudo astra-swapwiper-control enable Проверка состояния: sudo astra-swapwiper-control is-enabled enabled включен disabled выключен - установкой в конфигурационном файле /etc/parsec/swap_wiper.conf для параметра ENABLED значения Y.	
5	**Регистрация событий безопасности**		
	Управление аудитом		
5.1	Включение служб логирования syslog-ng и auditd	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности, выполняется запуск служб логирования syslog-ng и auditd. Включение службы логирования syslog-ng осуществляется: - с использованием графической утилиты «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения опции <Запуск службы логирования>. - с использованием консольной утилиты systemctl применением команды: sudo systemctl start syslog-ng	

№	Наименование настройки	Действия / Параметр	Мера
		Включение службы логирования auditd осуществляется: - с использованием консольной утилиты systemctl применением команды: sudo systemctl start auditd sudo systemctl enable auditd	
5.2	Включение PARSEC-аудита для файлов и процессов	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности, выполняется включение PARSEC-аудита для файлов и процессов. При включении PARSEC-аудита файл с правилами 10-parsec.rules, шаблон которого хранится в /usr/lib/parsec/audit/rules.d/, копируется в каталог /etc/audit/rules.d/. Значения в файлах /parsecfs/disable-all-audit, /parsecfs/disable-denied-audit и /parsecfs/disable-non-mac-audit изменяются на 0. Настройка осуществляется с использованием консольной утилиты astra-audit-control: sudo astra-audit-control enable Проверка состояния: sudo astra-audit-control is-enabled enabled включен disabled выключен Подсистема аудита может оказывать существенное влияние на производительность ОС.	
5.3	Включение сетевого PARSEC-аудита	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности, выполняется включение сетевого PARSEC-аудита. При включении сетевого PARSEC-аудита файл с правилами 10-parsec-nw.rules, шаблон которого хранится в /usr/lib/parsec/audit/rules.d/, копируется в каталог /etc/audit/rules.d/ и правила начинают выполняться. Настройка осуществляется с использованием консольной утилиты astra-audit-network-control: sudo astra-audit-network-control enable Проверка состояния: sudo astra-audit-network-control is-enabled enabled включен	

№	Наименование настройки	Действия / Параметр	Мера
		disabled выключен Сетевой аудит, как и подсистема аудита в целом, могут оказывать существенное влияние на производительность ОС. При необходимости возможно отключить сетевой PARSEC-аудит, что значительно уменьшит объем журналов регистрации сетевых событий. При выключении сетевого PARSEC-аудита файл /etc/audit/rules.d/10-parsec-nw.rules удаляется из каталога /etc/audit/rules.d/, в результате чего правила аудита перестают выполняться.	
Настройка ротации журналов			
5.4	Настройка ротации журнала /var/log/audit/audit.log	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности в течение установленного оператором времени хранения, выполняется настройка ротации журнала событий /var/log/audit/audit.log. Для настройки ротации журнала /var/log/audit/audit.log необходимо в файле /etc/audit/auditd.conf задать необходимые значения параметрам: log_file – указывается путь к файлу журнала. По умолчанию /var/log/audit/audit.log; freq – указывается частота регистрации. Будет осуществляться принудительная регистрация каждых <N> записей; max_log_file – максимальный размер файла, в Мб; max_log_file_action – действие, применяемое, когда размер журнала увеличится до максимального значения; num_logs – количество сохраняемых файлов журналов при ротации. Пример настройки /etc/audit/auditd.conf: log_file = /var/log/audit/audit.log freq = 1 max_log_file = 8 max_log_file_action = ROTATE num_logs = 5 Пример команд для настройки: sudo sed -Ei 's/log_file =.*/log_file = /var/log/audit/audit.log/g' /etc/audit/auditd.conf	РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		sudo sed -Ei 's/freq =.*/freq = 1/g' /etc/audit/auditd.conf sudo sed -Ei 's/max_log_file =.*/max_log_file = 8/g' /etc/audit/auditd.conf sudo sed -Ei 's/max_log_file_action =.*/max_log_file_action = ROTATE/g' /etc/audit/auditd.conf sudo sed -Ei 's/num_logs =.*/num_logs = 5/g' /etc/audit/auditd.conf	
5.5	Настройка ротации журнала /parsec/log/astra /events	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности в течение установленного оператором времени хранения, выполняется настройка ротации журнала событий безопасности /parsec/log/astra/events. Настройка осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» → «Настройки» → «Ротация основного лога» - путем активации опций: «Количество файлов» и установкой значения, «Максимальный размер файла» или «Период ротации» и установкой значений. - путем редактирования конфигурационного файла /etc/logrotate.d/syslog-ng-mod-astra. Для активации опции «Количество файлов» необходимо добавить в файл параметр rotate с необходимым значением. Для активации опции «Максимальный размер файла» необходимо добавить в файл параметр size с необходимым значением. Для активации опции «Период ротации» необходимо добавить в файл параметр daily или другой параметр. Пример настройки /etc/logrotate.d/syslog-ng-mod-astra: { rotate 12 size 25M missingok notifempty compress delaycompress	РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		sharedscripts prerotate chattr -a /parsec/log/astra/events > /dev/null endscript postrotate astra-protect-event-log > /dev/null invoke-rc.d syslog-ng reload > /dev/null endscript } Пример команд для замены значений: sed -i 's/\(\s*\)rotate [0-9]*/\1rotate 20/g' /etc/logrotate.d/syslog-ng-mod-astra sed -i 's/\(\s*\)size [0-9]*/\1size 25/g' /etc/logrotate.d/syslog-ng-mod-astra sed -i 's/\(size \).*M/\daily/g' /etc/logrotate.d/syslog-ng-mod-astra * Параметры «Максимальный размер файла» (size) и «Период ротации» (daily) не устанавливаются совместно.	
5.6	Настройка ротации системных журналов	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности в течение установленного оператором времени хранения, выполняется настройка ротации системных журналов. Настройка осуществляется путем конфигурирования файлов каталога /etc/logrotate.d/, содержащего конфигурацию Logrotate для всех установленных служб, которым требуется ротация.	РСБ.3
5.7	Настройка запуска службы Logrotate	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности в течение установленного оператором времени хранения, необходимо проверить, что служба Logrotate периодически запускается. Проверить файлы настроек ротации в одном из каталогов: /etc/cron.hourly /etc/cron.daily /etc/cron.monthly /etc/cron.weekly Конфигурационные файлы ротации всех системных журналов расположены в каталоге /etc/logrotate.d.	РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
5.8	Настройка действия admin_space_left при недостаточном месте на диске	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности, выполняется настройка выдачи предупреждения администратору при заполнении установленной оператором части (процента или фактического значения) объема памяти для хранения информации о событиях безопасности. Настройка оповещения производится с использованием: - графической утилиты «Конфигурация аудита» (system-config-audit) по пути: «Пуск» → «Параметры» → раздел «Безопасность» → «Регистрация событий и аудит» → «Конфигурация аудита» → «Конфигурация» → «Настройки» → «Мало дискового пространства» путём установки значений для параметров: «Первый порог» и выбором необходимой реакции; «Второй порог» и выбором необходимой реакции. - путем конфигурирования /etc/audit/auditd.conf и настройкой действия admin_space_left при недостаточном месте на диске. Файл должен содержать следующие строки: space_left = XX space_left_action = <одно из следующих значений: (ignore, syslog, email, exec, suspend, single, halt)> admin_space_left = YY admin_space_left_action = <одно из следующих значений: (ignore, syslog, email, exec, suspend, single, halt)> Пример команд для замены значений: sudo sed -Ei 's/space_left =.*/space_left = 80/g' /etc/audit/auditd.conf sudo sed -Ei 's/space_left_action =.*/space_left_action = SYSLOG/g' /etc/audit/auditd.conf sudo sed -Ei 's/admin_space_left =.*/admin_space_left = 50/g' /etc/audit/auditd.conf sudo sed -Ei 's/admin_space_left_action =.*/admin_space_left_action = SUSPEND/g' /etc/audit/auditd.conf	РСБ.4
Настройка регистрации событий			
5.9	Регистрация событий входа/выхода	Должна осуществляться регистрация событий входа/выхода субъектов доступа и загрузки (останова) ОС.	РСБ.1 РСБ.3 ОЦЛ.8

№	Наименование настройки	Действия / Параметр	Мера
	субъектов доступа и загрузки (останова) ОС	Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий: — «Идентификация и аутентификация субъекта доступа» — «Работа системы» Регистрация будет осуществляться в журнал /parsec/log/astra/events. - с использованием инструмента astra-admin-events: sudo astra-admin-events -G authorization --enable sudo astra-admin-events -G system-operation --enable	УПД.8
5.10	Регистрация событий запуска/завершения процессов	Должны регистрироваться события запуска/завершения процессов, связанных с обработкой защищаемой информации, в рамках сессии работы пользователей. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий из группы «События системы»: — «Запуск приложения или процесса» (данное событие порождает большой объем записей в логах) —«Завершение приложения или процесса» (данное событие порождает большой объем записей в логах) —«Процесс остановлен из-за нехватки памяти» —«Нештатное завершение приложения или процесса» Регистрация будет осуществляться в журнал /parsec/log/astra/events. - с использованием инструмента astra-admin-events: sudo astra-admin-events -E execute-process --enable sudo astra-admin-events -E process-ends --enable	РСБ.2 РСБ.3 ОЦЛ.8

№	Наименование настройки	Действия / Параметр	Мера
		sudo astra-admin-events -E process-out-of-ram --enable sudo astra-admin-events -E process-ends-abnormally --enable	
5.11	Регистрация событий работы подсистемы аудита	Должна осуществляться регистрация событий, связанных с работой подсистемы аудита. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий: – «События аудита» – «События самодиагностики подсистемы регистрации событий» – «Управление журналами (записями) регистрации событий безопасности» Регистрация будет осуществляться в журнал /parsec/log/astra/events. - с использованием инструмента astra-admin-events: sudo astra-admin-events -G audit --enable sudo astra-admin-events -G security-logs --enable sudo astra-admin-events -G self-diagnostics --enable	РСБ.1 РСБ.3 АНЗ.3 АНЗ.5
5.12	Регистрация событий изменения привилегий учетных записей	Должна осуществляться регистрация событий, связанных с изменениями привилегий учетных записей. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для группы событий: – «Управление привилегиями пользователя» Регистрация будет осуществляться в журнал /parsec/log/astra/events. - с использованием инструмента astra-admin-events: sudo astra-admin-events -G capabilities-change --enable	РСБ.1 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
5.13	Регистрация по использованию полномочий по изменению атрибутов доступа к файлам	Должна осуществляться регистрация по использованию полномочий по изменению доступа к файлам. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий: — «Управление атрибутами доступа» (как минимум событий «Вызов chown», «Вызов chmod», «Изменение ACL», «Вызов umask») — «Управление мандатными атрибутами» Данные события могут порождать большой объем записей в логе. Регистрация будет осуществляться в журнал /parsec/log/astra/events. - с использованием инструмента astra-admin-events: sudo astra-admin-events -E event-chown --enable sudo astra-admin-events -E event-chmod --enable sudo astra-admin-events -E event-acl --enable sudo astra-admin-events -E event-umask --enable sudo astra-admin-events -G mac --enable	РСБ.1 РСБ.3 АНЗ.5
5.14	Регистрация изменений статуса объектов, попыток доступа к защищаемым объектам	Должна осуществляться регистрация изменений статуса защищаемых объектов. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий из группы «События безопасности»: — «Удаление файла» — «Изменение файла» — «Открытие файла» — «Создание файла» — «Переименование файла»	РСБ.1 АНЗ.3 ОЦЛ.8

№	Наименование настройки	Действия / Параметр	Мера
		– «Изменение каталога или его содержимого» с указанием в параметрах для поиска событий значения ключей для поиска записи в логе (указанием подвергаемого контролю файла). Регистрация будет осуществляться в журнал /parsec/log/astra/events. - с использованием инструмента astra-admin-events: sudo astra-admin-events -E file-removal --enable sudo astra-admin-events -E modifying-file --enable sudo astra-admin-events -E file-opened --enable sudo astra-admin-events -E file-created --enable sudo astra-admin-events -E file-renamed --enable sudo astra-admin-events -E modifying-directory --enable Указание на подвергаемый контролю файл для событий modifying-file, modifying-directory, file-opened выполняется с использованием аргумента -P. Например, чтобы указать объект контроля для события modifying-file, необходимо выполнить команду с указанием пути к файлу для "/path/to/file": sudo astra-admin-events -E modifying-file -P 'filter-values' '.auditd.key' '["/path/to/file"]' Регистрация будет осуществляться в журнал /var/log/audit/audit.log.	
5.15	Регистрация изменения параметров и настроек системного ПО	Должна осуществляться регистрация изменения параметров и настроек системного программного обеспечения. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий: – «Изменение настроек общего программного обеспечения» – «Установка, изменение системного времени» А также событий из группы «События безопасности»: – «Изменение файла» – «Изменение каталога или его содержимого»	РСБ.1 АНЗ.3 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		с указанием в параметрах для поиска событий значения ключей для поиска записи в логе (указанием подвергаемого контролю файла). Регистрация будет осуществляться в журнал /parsec/log/astra/events. - с использованием инструмента astra-admin-events: sudo astra-admin-events -G general-software --enable sudo astra-admin-events -G system-time --enable sudo astra-admin-events -G ммodifying-file --enable sudo astra-admin-events -G modifying-directory --enable Регистрация будет осуществляться в журнал /var/log/audit/audit.log.	
5.16	Регистрация изменения параметров средств защиты информации	Должна осуществляться регистрация изменения параметров и настроек средств защиты информации. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации группы событий: – «Изменение параметров настроек средств защиты информации» – - с использованием инструмента astra-admin-events: sudo astra-admin-events -G safepolicy --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 АНЗ.3 РСБ.3
5.17	Регистрация подключения и отключения внешних устройств, в том числе через шину USB	Должна осуществляться регистрация подключения внешних устройств, в том числе через шину USB. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка	РСБ.1 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		регистрации системных событий» путем включения регистрации событий из группы «События системы»: – «Устройство подключено» – «Обнаружено устройство хранения данных USB» – «Монтирование машинного носителя информации» – «Устройство отключено» – «Размонтирован машинный носитель информации» – "Запрет монтирования машинного носителя непривилегированным пользователем» - с использованием инструмента astra-admin-events: sudo astra-admin-events -E new-usb-device --enable sudo astra-admin-events -E usb-disconnect --enable sudo astra-admin-events -E usb-mass-storage-detected --enable sudo astra-admin-events -E device-mount --enable sudo astra-admin-events -E device-unmount --enable sudo astra-admin-events -E device-mount-attempt-blocked --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.18	Запись дополнительной информации о событиях безопасности, включающей полнотекстовую запись привилегированных команд	Должна осуществляться запись дополнительной информации о событиях безопасности, включающей полнотекстовую запись привилегированных команд. Система аудита должна записывать действия администратора для всех пользователей sudo, включая суперпользователя. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий: – «Запуск приложения или процесса от имени суперпользователя»	РСБ.1 РСБ.2 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		- с использованием инструмента astra-admin-events: sudo astra-admin-events -E execute-sudo-process --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events. При необходимости установить и настроить библиотеку Snoopy, позволяющую записывать в журнал /var/log/syslog все запущенные команды вместе с их аргументами. sudo apt-get install snoopy Управление конфигурацией библиотеки осуществляется в файле конфигурации /etc/snoopy.ini	
5.19	Регистрация изменения аппаратной конфигурации СВТ, на котором функционирует ОС, и состава установленного ПО.	Должна осуществляться регистрация изменения аппаратной конфигурации СВТ, на котором функционирует ОС, и состава установленного ПО. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий: – «События управления программными пакетами» – «События системы» (такие как «Устройство подключено», «Обнаружено устройство хранения данных USB», «Смонтирован машинный носитель информации», «Устройство отключено», «Размонтирован машинный носитель информации») - с использованием инструмента astra-admin-events: sudo astra-admin-events -G packages --enable sudo astra-admin-events -E new-usb-device --enable sudo astra-admin-events -E usb-disconnect --enable sudo astra-admin-events -E usb-mass-storage-detected --enable sudo astra-admin-events -E device-mount --enable sudo astra-admin-events -E device-unmount --enable sudo astra-admin-events -E device-mount-attempt-blocked --enable	РСБ.1 РСБ.3 АН3.4

№	Наименование настройки	Действия / Параметр	Мера
		Регистрация будет осуществляться в журнал /parsec/log/astra/events. Для вывода списка оборудования и информации об устройствах рекомендуется инсталлировать утилиту: sudo apt install lshw Проверить аппаратную конфигурацию СВТ можно с помощью команды: sudo lshw	
5.20	Запись событий об изменении информации о пользователях/ группах	Должна осуществляться регистрация событий об изменении информации о пользователях/группах и всех действий по управлению учётными записями пользователей. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий: – «События управления учетными записями пользователей» – «События управления группами пользователей» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G user-accounting --enable sudo astra-admin-events -G user-groups --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.3 РСБ.1
5.21	Запись событий изменения системного сетевого окружения	Должна осуществляться регистрация событий изменения системного сетевого окружения. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения	АНЗ.3

№	Наименование настройки	Действия / Параметр	Мера
		регистрации для группы событий: – «Изменение в сетевой адресации» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G network-addressing --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.22	Запись событий об исчерпании ресурсов системы	Должна осуществляться регистрация событий об исчерпании ресурсов системы. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для группы событий: – «События ресурсов системы» – а также события «Процесс остановлен из-за нехватки памяти» из группы событий «События системы» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G resources --enable sudo astra-admin-events -E process-out-of-ram --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	ОДТ.1
5.23	Запись событий об удалении файлов пользователем	Должен осуществляться контроль действий по удалению защищаемой информации. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий: – «Удаление файла»	РСБ.1 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		– «Журнал аудита удалён» – «Журнал событий удалён» - с использованием инструмента astra-admin-events: sudo astra-admin-events -E file-removal --enable sudo astra-admin-events -E audit-log-removed --enable sudo astra-admin-events -E events-log-removed --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.24	Регистрация событий о загрузке и выгрузке модулей ядра	Должна осуществляться регистрация событий о загрузке и выгрузке модулей ядра. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий из группы «События системы»: – «Загрузка или выгрузка модуля ядра» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G kernel-module --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 АН3.4 РСБ.3
5.25	Регистрация блокирования пользователя	Должна осуществляться регистрация событий блокирования пользователя. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий из группы «События безопасности»: – «Учетная запись заблокирована по истечении количества попыток ввода пароля»	РСБ.1 РСБ.3 АН3.5

№	Наименование настройки	Действия / Параметр	Мера
		- с использованием инструмента astra-admin-events: sudo astra-admin-events -E user-blocked-by-tally --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.26	Регистрация смены аутентифицирующей информации учётных записей	Должна осуществляться регистрация событий смены аутентифицирующей информации учётных записей. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий из группы «События управления учетными записями пользователей»: – «Изменение наименования учетной записи» – «Смена пользовательского пароля» - с использованием инструмента astra-admin-events: sudo astra-admin-events -E changing-account-name --enable sudo astra-admin-events -E changing-account-password --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 РСБ.3 АНЗ.5
5.27	Регистрация выдачи печатных (графических) документов на твёрдую копию	Должна осуществляться регистрация событий выдачи печатных (графических) документов на твёрдую копию. Аудит событий выдачи печатных (графических) документов на бумажный носитель осуществляется в системных журналах /var/log/cups/page_log и/var/spool/cups/parsec. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий:	РСБ.1 РСБ.3 ОЦЛ.5

№	Наименование настройки	Действия / Параметр	Мера
		— «Вывод информации на печать, в том числе защищенной» — «Пользовательские события («Задание ожидает печати», «Задание промаркировано», «Задание в процессе печати» и др.) - с использованием инструмента astra-admin-events: sudo astra-admin-events -G printing --enable sudo astra-admin-events -G custom-events --enable Регистрация, будет осуществляться в журнал /parsec/log/astra/events.	
5.28	Регистрация нарушения целостности контролируемых исполняемых модулей и файлов данных	Должна осуществляться регистрация нарушения целостности контролируемых исполняемых модулей и файлов данных. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий из группы «События безопасности»: — «Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG)» - с использованием инструмента astra-admin-events: sudo astra-admin-events -E unsigned-binary-file --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events. Регистрация событий постановки/снятия с контроля целостности исполняемых модулей и файлов данных, а также событий неуспешного запуска неподписанных файлов осуществляется в системном журнале /var/log/kern.log и ksystemlog. Регистрация событий, связанных с работой регламентного контроля целостности, осуществляется в журнале /var/log/afick.log.	РСБ.1 РСБ.3 АНЗ.3

№	Наименование настройки	Действия / Параметр	Мера
5.29	Регистрация событий, связанных с использованием сетевых соединений	В ОС должна осуществляться регистрация событий, связанных с установлением и разрывом сетевых соединений (в том числе беспроводных), для выявления попыток несанкционированного подключения и выявления возможных инцидентов. Настройка регистрации событий, связанных с использованием соединений, осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для группы событий: — «События сети» (регистрация события «Событие сети» из данной группы порождает большой объем логов, поэтому его включение осуществляется на усмотрение администратора) - с использованием инструмента astra-admin-events: sudo astra-admin-events -G network --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	ЗИС.11 ЗИС.20
5.30	Регистрация попыток удаленного доступа	В ОС должна осуществляться регистрация попыток удаленного доступа. Настройка регистрации событий удаленного доступа осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации событий из группы «События сети» и группы «Идентификация и аутентификация субъекта доступа»: — «Установка сетевого соединения» — «Сетевое соединение установлено» — «Сетевое соединение недоступно» — «Установлено соединение с Интернетом» — «Разрыв сетевого соединения»	РСБ.1 РСБ.3 УПД.13

№	Наименование настройки	Действия / Параметр	Мера
		– «Неуспешная авторизация» – «Успешный вход в систему» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G network --enable sudo astra-admin-events -E failed-authorization --enable sudo astra-admin-events -E successed-authorization --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.31	Регистрация событий, связанных с доступом субъектов доступа к компонентам виртуальной инфраструктуры	Должна осуществляться регистрация событий, связанных с доступом субъектов доступа к компонентам виртуальной инфраструктуры. Настройка регистрации осуществляется с использованием (при условии установленного пакета astra-kvm-secure): - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий: – «Доступ пользователей средства виртуализации к ВМ» – «Управление контрольными точками ВМ» – «Изменение состояние виртуальных машин» – «Управление запуском/остановкой компонент средства виртуализации» – «Управление виртуальными машинами» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G libvirtd-access-messages --enable sudo astra-admin-events -G libvirtd-controlcheckpointVM-messages --enable sudo astra-admin-events -G libvirtd-changestateVM-messages --enable sudo astra-admin-events -G libvirtd-system-messages --enable sudo astra-admin-events -G libvirtd-controlVM-messages --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	ЗСВ.3

№	Наименование настройки	Действия / Параметр	Мера
5.32	Регистрация событий, связанных с изменением в составе и конфигурации компонентов виртуальной инфраструктуры	Должна осуществляться регистрация событий, связанных с изменением в составе и конфигурации компонентов виртуальной инфраструктуры. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для групп событий: – «Изменение конфигурации средства виртуализации» – «Изменение конфигурации виртуального коммутатора» – «Изменение конфигураций виртуальных машин» – «Изменение конфигурации дискового хранилища» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G libvirtd-config-messages --enable sudo astra-admin-events -G libvirtd-network-messages --enable sudo astra-admin-events -G libvirtd-changeconfigVM-messages --enable sudo astra-admin-events -G libvirtd-storage-messages --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	ЗСВ.3
5.33	Регистрация событий, связанных с изменением правил разграничения доступа к компонентам виртуальной инфраструктуры	Должна осуществляться регистрация событий, связанных с изменением правил разграничения доступа к компонентам виртуальной инфраструктуры. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения	ЗСВ.3

№	Наименование настройки	Действия / Параметр	Мера
		регистрации для групп событий: – «Управление атрибутами доступа» – «Изменение ролевой модели» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G libvirtd-accesschange-messages --enable sudo astra-admin-events -G libvirtd-polkit-messages --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.34	Регистрация событий, связанных с перемещением и размещением виртуальных машин	Должна осуществляться регистрация событий, связанных с перемещением и размещением виртуальных машин. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения регистрации для группы событий: – «Перемещение виртуальных машин» - с использованием инструмента astra-admin-events: sudo astra-admin-events -G libvirtd-migrateVM-messages --enable Регистрация будет осуществляться в журнал /parsec/log/astra/events.	ЗСВ.3
Настройка оповещений			
5.35	Включение оповещений событий безопасности	Должно осуществляться оповещение администратора безопасности о событиях безопасности. В системе должна быть установлена программа «Центр уведомлений». Если ее нет, то ее установка осуществляется командой: sudo apt install fly-notifications sudo /usr/share/syslog-ng-mod-astra/generate-notifyrc Настройка оповещений на появление событий безопасности осуществляется с использованием: - графического инструмента «Настройка регистрации	УПД.1 УПД.8 АНЗ.3 ОДТ.1 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		системных событий» (astra-systemsettings fly-admin-events) по пути: «Пуск» →«Параметры» →раздел «Безопасность» → «Регистрация событий и аудит» → «Настройка регистрации системных событий» путем включения отправки уведомлений (правой кнопкой машины нажать в сроке события и в контекстном меню выбрать «Включить отправку уведомлений», далее «Отправлять уведомления только администраторам») для событий: – «Создание учетной записи пользователя» – «Учетная запись заблокирована по истечении количества попыток ввода пароля» – «Удаление учетной записи пользователя» – «Успешный вход в систему» – «Неуспешная авторизация» – «Выход из системы» – «Система загружена» – «Система выключена» – «Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG)» – событий группы «Изменение параметров настроек средств защиты информации» – событий группы «Изменение настроек общего программного обеспечения» – «Нештатное завершение приложения или процесса» – «Критическая ошибка подсистемы регистрации событий» – «Ошибка подсистемы регистрации событий» – «Разрыв сетевого соединения» – «Сетевое соединение недоступно» – «Недостаточно свободного дискового пространства в каталоге» – «Дисковая квота близка к исчерпанию или исчерпана» – «Недостаточно свободной оперативной памяти» – «Процесс остановлен из-за нехватки памяти» – событий группы «Пользовательские события» - путем создания в каталоге /etc/syslog-ng/conf.d/ конфигурационных файлов уведомлений. Для каждого вышеуказанного события необходимо в каталоге /etc/syslog-ng/conf.d/ создать файлы mod-astra-<event-	

№	Наименование настройки	Действия / Параметр	Мера

		id>.conf со следующим содержимым:
		filter astra_<event-id>_filter {
		match("^<event-id>$" value("MSG.astra-audit.message_id"));
		};
		
		destination astra_<event-id>_dbus_dst {
		python(
		
		class("syslog_ng_mod_astra.astra_syslog_ng_destination.AstraSyslogNgDestination")
		options("destination_type", "dbus"
		"message_type", "audit"
		"event_user", "@all"
		"event_group", "astra-admin"
		"event_id", "<id события>"
		"event_title", "<наименование события на русском языке>"
		"event_icon", ""
		"event_params", ""
		"event_format", "")
		persist-name("<event-id>")
		);
		};
		
		log {
		source(astra_events_src);
		parser(astra_events_parser);
		filter(astra_<event-id>_filter);
		destination(astra_<event-id>_dbus_dst);
		};
		
		Данное содержимое файла общее для всех событий. Для каждого события необходимо изменить <event-id>, <наименование события на русском языке> и <id события> на идентификационные значения события.	

Настройка централизованного сбора журналов			
5.36	Использование средств централизованного протоколирова	Централизованное автоматизированное управление сбором, записью, хранением информации о событиях безопасности, а также просмотр и анализ информации о действиях пользователей, мониторинг (просмотр, анализ) результатов регистрации событий безопасности,	РСБ.3 РСБ.4 РСБ.5 РСБ.7 РСБ.8

№	Наименование настройки	Действия / Параметр	Мера
	ния zabbix	осуществляется с помощью средств централизованного протоколирования и аудита событий безопасности. Установка и настройка системы мониторинга Zabbix осуществляется в соответствии с положениями документа «Руководство администратора. Часть 1» п. «Средства централизованного протоколирования и аудита» и с использованием инструкций: https://wiki.astralinux.ru/x/kgH1AQ	ОДТ.1 ОДТ.3 ОЦЛ.8 УПД.9 АНЗ.4. АНЗ.5 ЗИС.7 ЗСВ.3 ЗСВ.4
Настройка синхронизации времени			
5.37	Настройка синхронизации времени	С целью реализации мер, направленных на осуществление синхронизации системного времени выполняется настройка синхронизации времени в соответствии положениями документа «Руководство администратора. Часть 1» п. «Службы точного времени». В рамках настройки необходимо определить источник надежных меток времени и установить периодичность синхронизации системного времени. Настройка осуществляется с использованием: - графического инструмента «Синхронизация времени» (fly-admin-time) по пути: «Пуск» →«Настройки» →раздел «Безопасность» → «Регистрация событий и аудит» → «Синхронизация времени» путем активации работы выбранной службы синхронизации, выбором сервера синхронизации и установкой интервала синхронизации в расширенных настройках. Рекомендуемый список серверов для синхронизации времени: ntp1.vniiftri.ru ntp2.vniiftri.ru ntp3.vniiftri.ru ntp4.vniiftri.ru - в случае использования службы systemd-timesyncd путем редактирования конфигурационного файла службы timesyncd /etc/systemd/timesyncd.conf. Задаются значения для параметров RootDistanceMaxSec («Максимальная дистанция для корневых часов»), PollIntervalMaxSec («Максимальный интервал между опросами»), PollIntervalMinSec («Минимальный интервал между опросами») и NTP («Список серверов для	РСБ.6

№	Наименование настройки	Действия / Параметр	Мера
		синхронизации») Пример конфигурации: [Time] PollIntervalMaxSec=2048 PollIntervalMinSec=32 RootDistanceMaxSec=5 NTP=vniiftri2.khv.ru ntp4.vniiftri.ru ntp3.vniiftri.ru ntp21.vniiftri.ru ntp2.vniiftri.ru ntp2.niiftri.irkutsk.ru ntp1.vniiftri.ru - в случае использования службы chrony путем редактирования конфигурационного файла службы chrony /etc/chrony/chrony.conf. Задаются значения для параметров server (указывается сервер синхронизации), maxupdateskew («Максимальное искажение для обновления»), rtcsync (использование директивы rtcsync), makestep («Настройка коррекции шагом» с указанием порога и предела). Пример конфигурации: server ntp3.vniiftri.ru iburst server ntp4.vniiftri.ru iburst server ntp21.vniiftri.ru iburst server vniiftri2.khv.ru iburst server ntp2.niiftri.irkutsk.ru iburst server ntp1.vniiftri.ru iburst server ntp2.vniiftri.ru iburst maxupdateskew 100.0 rtcsync makestep 1 3	
6	**Обеспечение целостности**		
Тестирование СЗИ			
6.1	Тестирование СЗИ	В установленный период администратором должно проводиться тестирование всех функций СЗИ от НСД с помощью специальных программных средств, имитирующих попытки НСД. В состав ОС входят средства тестирования функций СЗИ от НСД, находящиеся в каталоге /usr/lib/parsec/tests. Данный набор обеспечивает тестирование механизмов	ОЦЛ.1 АН3.3

№	Наименование настройки	Действия / Параметр	Мера
		безопасности из состава ОС, включая проверки: – дискреционного управления доступом к объектам ФС; – мандатного управления доступом к объектам ФС, IPC и при сетевых взаимодействиях; – подсистемы регистрации событий; – механизма защиты памяти и изоляции процессов; – механизма очистки памяти; – механизма привилегий процесса. В состав ОС входят средства тестирования функций СЗИ СУБД, обеспечивающие тестирование всех функций СЗИ СУБД, включая управление доступом, регистрацию событий, идентификацию и аутентификацию, контроль целостности, очистку памяти, надежное восстановление, регистрацию событий и др. Для этого используется пакет postgresql-se-test-x.x. Перед проведением тестирования система должна быть выведена из эксплуатации, т. к. в процессе тестирования меняются параметры работы средств защиты информации, параметры объектов и субъектов доступа, что может вызвать ошибки и сбои в работе системного и прикладного ПО, угрозы нарушения конфиденциальности и доступности информации. После завершения тестирования все параметры возвращаются в исходное состояние, и система может быть введена в эксплуатацию. Тестирование проводится в соответствии с документом «Руководство по КСЗ. Часть 2» Для запуска автоматической процедуры тестирования подсистемы безопасности PARSEC необходимо: 1) войти в систему от имени администратора; 2) перейти в каталог /usr/lib/parsec/tests: cd /usr/lib/parsec/tests 3) осуществить запуск скрипта: sudo ./run.sh (или с опцией -v для режима подробного вывода сообщений). При этом на экране монитора будут появляться сообщения о прохождении и результатах выполнения тестов. Подробная информация о результатах тестирования будет записана в файл tests.log, находящийся	

№	Наименование настройки	Действия / Параметр	Мера
		в каталоге /usr/lib/parsec/tests. Для запуска автоматической процедуры тестирования СУБД необходимо: 1) войти в систему от имени администратора с высокой меткой целостности; 2) запустить окно терминала; 3) установить пакет тестирования выбранной версии СУБД командой: sudo apt install postgresql-se-test-x.x 4) установить на каталог /tmp необходимые для выполнения тестирования мандатные атрибуты: sudo pdpl-file 3:0:-1:ccnr /tmp 5) перейти в каталог /usr/share/postgresql/x.x/test/pgacext/ командой: cd /usr/share/postgresql/x.x/test/pgacext/ 6) запустить тесты командой: sudo ./runtests -all 7) сбросить мандатные атрибуты каталога /tmp: sudo pdpl-file 0 /tmp	
Регламентный контроль целостности			
6.2	Настройка контроля целостности с использованием средства Afick	Регламентный контроль проверяет целостность и неизменность ключевых системных файлов, сравнивая их контрольные суммы с эталонными значениями. На контроль целостности должны быть поставлены подлежащие защите исполняемые модули и файлы данных: – программного обеспечения средств защиты информации, включая их обновления; – критически важные бинарные и конфигурационные файлы операционной системы и прикладного ПО; – файлы образа ядра и загрузчика ОС; – архивные файлы, параметры настройки средств защиты информации и ПО и иные данные, не подлежащие изменению в процессе обработки информации; – исполняемые файлы компонентов программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники. Настройка регламентного контроля целостности	АНЗ.3 АНЗ.4 ОЦЛ.1 ОЦЛ.2 ЗИС.15 ЗИС.18 ОПС.2

№	Наименование настройки	Действия / Параметр	Мера
		выполняется в конфигурационном файле /etc/afick.conf, в котором необходимо указать пути к файлам/каталогам, подвергаемым контролю целостности, и правила контроля целостности, применяемые к файлам и каталогам. Пример настройки: echo '/boot/vmlinuz-* PARSEC' >> /etc/afick.conf echo '/boot/initrd.img-* PARSEC' >> /etc/afick.conf echo '/boot/grub/grub.cfg PARSEC' >> /etc/afick.conf echo '/etc/X11/default-display-manager PARSEC' >> /etc/afick.conf echo '/etc/exports PARSEC' >> /etc/afick.conf echo '/etc/fstab PARSEC' >> /etc/afick.conf echo '/etc/group PARSEC' >> /etc/afick.conf echo '/etc/init.d/ PARSEC' >> /etc/afick.conf echo '/etc/inittab PARSEC' >> /etc/afick.conf echo '/etc/pam.d PARSEC' >> /etc/afick.conf echo '/etc/passwd PARSEC' >> /etc/afick.conf echo '/etc/rc* PARSEC' >> /etc/afick.conf echo '/etc/securetty PARSEC' >> /etc/afick.conf echo '/etc/shells PARSEC' >> /etc/afick.conf echo '/etc/sysctl.conf PARSEC' >> /etc/afick.conf echo '/lib/modules/*/misc/digsig_verif.ko PARSEC' >> /etc/afick.conf echo '/lib/modules/*/misc/parsec.ko PARSEC' >> /etc/afick.conf echo '/lib/modules/*/misc/parsec-cifs.ko PARSEC' >> /etc/afick.conf echo '/lib/security/pam PARSEC' >> /etc/afick.conf echo '/bin/ PARSEC' >> /etc/afick.conf echo '/sbin/ PARSEC' >> /etc/afick.conf echo '/usr/bin/ PARSEC' >> /etc/afick.conf echo '/usr/sbin/ PARSEC' >> /etc/afick.conf После внесение изменений создать базу контрольных сумм и атрибутов при помощи команды: afick -i При запуске AFICK автоматически установит ежедневное задание для CRON. Файл с заданием находится в /etc/cron.daily/afick_cron. В случае, если функциональные возможности	

№	Наименование настройки	Действия / Параметр	Мера
		информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.	
6.3	Исключение возможности использования средств разработки и отладки программного обеспечения	Администратором должна быть исключена возможность использования средств разработки и отладки программного обеспечения во время обработки и (или) хранения информации в целях обеспечения целостности программной среды. Исключение из Astra Linux средств разработки и отладки программ осуществляется администратором с помощью инструментов управления пакетами и средствами ограничения программной среды.	ОЦЛ.1

*Для отдельных компонент из состава дистрибутива ОС (браузер, офисные пакеты, СУБД, web-сервера, сервер печати и пр.) разрабатываются собственные конфигурации безопасности.