Согласовано ФСТЭК России
от 31.01.2024 г.

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

(Листов - 85)

Москва
2023

СОДЕРЖАНИЕ

АННОТАЦИЯ

Настоящий документ содержит общие рекомендации по настройке безопасных конфигураций параметров безопасности операционной системы специального назначения «Astra Linux Special Edition» (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 СДЗ 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 средствами СДЗ

№	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).
4.	Раздел ESP	Контролировать целостность данного раздела необходимо в случае использования таблицы

№	Объект контроля целостности	Примечание
		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.conf	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 ЗПС 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, отвечающие за загрузки 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. Наличие у злоумышленника доступа к настройкам BIOS позволяет разрешить загрузку с компакт-диска или флэш-накопителя со сторонней ОС (Live CD), войти в режим восстановления или однопользовательский режим, что, в свою очередь, позволит запускать произвольные процессы в системе или копировать конфиденциальные данные.

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 и соблюдения 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 WiFi. 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 и (при использовании пакета resolvconf) - для автоматизации автоматической перенастройки мобильных компьютеров, переключающихся между разными сетями. При стандартной установке Astra Linux эта служба 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. При переходе к использованию службы networking лучше отключить NetworkManager для избежание возможных конфликтов в части управления /etc/resolv.conf

– с использованием службы systemd-networkd / systemd-resolved. Современные службы 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. Данный инструмент рекомендуется использовать на этапе установки системы. 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 настройка в том числе 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 и 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» - «Панель управления» - «Прочее» - «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 (например, контроль несанкционированного подключения к ЛВС в пределах контролируемой зоны, защищенная передача сетевого трафика за пределами контролируемой зоны). Обеспечение защиты информации при межсетевом доступе (через внешние информационно-телекоммуникационные сети) реализуется сертифицированными криптографическим средствами защиты, предназначенными для построения виртуальных частных сетей.

В случае наличия средств удаленного администрирования и беспроводных системы передачи данных должны быть предприняты меры по нейтрализации возможностей реализации атак и скрытых каналов передачи данных согласно действующего законодательства РФ, нормативных и методических документов ФСТЭК России.

2. УКАЗАНИЯ ПО УСТАНОВКЕ, ОБНОВЛЕНИЮ И РЕЗЕРВНОМУ КОПИРОВАНИЮ ОС

2.1. Рекомендации по установке

Пароль для учетной записи администратора

В окне «Настройка учетных записей и паролей» программы установки осуществляется создание учетной записи администратора и задание пароля в соответствии с определяемыми администратором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов.

Рекомендации по настройке разделов

Разметка дисков осуществляется в окне «Разметка дисков» программы установки. Высокоуровневые системные каталоги рекомендуется располагать на раздельных физических разделах или логических томах. Общие принципы работы с физическими разделами или томами изложены ниже.

При установке ОС с уже существующей разметкой диска, необходимо выбирать опцию «Просмотр и изменение структуры разделов». После этого необходимо создать дополнительные логические тома внутри уже созданной группы томов. В общем случае, использование логических томов предпочтительнее использованию разделов, т.к. они позднее могут быть легко модифицированы.

При установке ОС с произвольной разметкой диска, рекомендуется создать отдельные тома или разделы для следующих высокоуровневых системных каталогов: /boot, /home, /var, /var/log, /var/log/audit, /tmp и /var/tmp, а также раздел для swap (при обоснованной необходимости).

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 2.1.

Таблица 2.1 - Рекомендации на настройке разделов

Раздел	Описание	Рекомендации по установке/настройке
/	Корневой раздел	Можно применять защитное преобразование (при условии,

Раздел	Описание	Рекомендации по установке/настройке
		что каталог /boot размещён в отдельном дисковом разделе).
/boot	Является первым разделом, который читается системой во время загрузки. В этом разделе хранятся образы загрузчика и образы ядра, которые используются для загрузки ОС Linux	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, избегать переполнения системного раздела (/boot) и также делает удобным частое резервное копирование пользовательских данных.	Можно применять защитное преобразование.
/tmp	Разделы /tmp и /var/tmp/ используются для хранения временных пользовательских данных и служебных данных системы	Можно применять защитное преобразование. При размере раздела /tmp менее 250МБ весьма вероятно возникновение ошибок при работе с графикой или с большими объёмами данных.
/var	Раздел содержит каталоги для хранения данных аудита /var/log, /var/log/audit	Можно применять защитное преобразование.
/var/tmp	Разделы /tmp и /var/tmp/ используются для хранения временных пользовательских данных и служебных данных системы	Можно применять защитное преобразование. В отличие от каталога /var подкаталог /var/tmp рекомендуется монтировать с опциями noexec,nodev,nosuid.
swap	Служебный раздел для хранения временных файлов, создаваемых системой для расширения оперативной памяти. При работе с конфиденциальной информацией использовать раздел подкачки не рекомендуется. В любой	Если необходимо использовать - то использовать с включенным защитным преобразованием, с включенным гарантированным удалением и очисткой разделов страничного обмена.

Раздел	Описание	Рекомендации по установке/настройке
	момент после установки ОС в качестве раздела подкачки можно назначить и использовать дисковый файл, однако, если раздел подкачки необходим, устанавливая ОС следует зарезервировать свободное место при разметке диска.	

Выбор уровня защищенности

В окне «Дополнительные настройки ОС» программы установки осуществляется выбор уровня защищенности ОС. Выбор уровня защищённости (варианта лицензирования) ОС необходимо обосновывать исходя из результатов анализа возможностей ОС по реализации базовых мер защиты и возможностей по нейтрализации актуальных угроз безопасности информации.

Таблица 2.2 - Общие рекомендации по выбору уровня защищенности

№ п/п	Наименование уровня защищенности	Описание
1.	Уровень защищенности «Базовый» (вариант лицензирования «Орел»)	Функциональные возможности базового варианта подходят* для обработки и защиты информации в информационных системах 3 класса защищенности (ГИС), информационных системах персональных данных 3-4 уровня защищенности (ИСПДн) и значимых объектов критической информационной инфраструктуры (КИИ). * возможно только в случае применения варианта лицензирования «Орел»: Astra Linux 1.7, вариант РУСБ.10015-01, уровень защищенности «Базовый». В случае применения Astra Linux 1.7 РУСБ.10015-10 - вариант лицензирования «Орел» может применяться только в системах, не обрабатывающих информацию, подлежащую защите в соответствии с законодательством Российской Федерации.
2.	Уровень защищенности «Усиленный» (вариант лицензирования «Воронеж»)	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.	Уровень защищенности «Максимальный» (вариант лицензирования «Смоленск)	Режим максимальной защищенности обеспечивает защиту информации, содержащей государственную тайну любой степени секретности и предназначен для обработки информации любой категории доступа в ГИС, в ИСПД, в составе значимых объектов КИИ, в иных информационных

№ п/п	Наименование уровня защищенности	Описание
		(автоматизированных) системах, обрабатывающих информацию ограниченного доступа, в т.ч. содержащую сведения, составляющие государственную тайну до степени секретности «особой важности» включительно.

После выбора уровня защищенности отобразится перечень функций безопасности ОС, соответствующий выбранному уровню. На каждом уровне доступны к использованию функции безопасности предыдущего уровня.

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
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
Очистка освобождаемой внешней памяти	При выборе данного пункта будет включен режим очистки блоков ФС непосредственно при их освобождении, а также режим очистки разделов страничного обмена. По умолчанию пункт не выбран (доступен для усиленного уровня защищенности).	Не используется на этапе установки/первичной настройки. Рекомендуется к включению при вводе системы в эксплуатацию
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	Не используется на этапе установки/первичной настройки.

Функция	Описание	Рекомендация
	пункт не выбран.	Рекомендуется к включению при вводе системы в эксплуатацию)
Запрет трассировки ptrace	При выборе данного пункта будет выключена возможность трассировки и отладки выполнения программного кода. По умолчанию пункт выбран.	Не используется на этапе установки/первичной настройки. Включается по решению администратора при вводе системы в эксплуатацию
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
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.	Не используется на этапе установки/первичной настройки. Рекомендуется к включению при вводе системы в эксплуатацию
Запрет исполнения скриптов пользователя	При выборе данного пункта будет блокировано интерактивное использование пользователем интерпретаторов. По умолчанию пункт не выбран.	Не используется на этапе установки/первичной настройки. Рекомендуется к включению при вводе системы в эксплуатацию
Запрет исполнения макросов пользователя	При выборе данного пункта будет блокировано исполнение макросов в стандартных приложениях. По умолчанию пункт не выбран.	Не используется на этапе установки/первичной настройки. Рекомендуется к включению при вводе системы в

Функция	Описание	Рекомендация
		эксплуатацию
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.	Не используется на этапе установки/первичной настройки. Рекомендуется к включению при вводе системы в эксплуатацию
Системные ограничения ulimits	При выборе данного пункта будут включены системные ограничения, установленные в файле /etc/security/limits.conf. По умолчанию пункт не выбран.	Не используется на этапе установки/первичной настройки. Рекомендуется к включению при вводе системы в эксплуатацию
Запрет автонастройки сети	При выборе данного пункта будет выключена автоматическая настройка сети в процессе установки ОС, сеть необходимо будет настроить вручную в соответствии с рекомендациями настоящего руководства. По умолчанию пункт не выбран.	Рекомендуется к включению
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

Установка пароля на системный загрузчик GRUB

В окне «Установка системного загрузчика GRUB на жёсткий диск» выполняется установка пароля на системный загрузчик в соответствии с определяемыми администратором 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. Первичная настройка ОС

Непосредственно после установки ОС (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. 17.2).

2.3. Отключение неиспользуемых сервисов и аппаратных устройств

Основными принципами настройки безопасности общесистемного и прикладного программного обеспечения в информационных и автоматизированных системах, являются:

1) Удаление или отключение неиспользуемого и наиболее подверженного уязвимостям ПО и аппаратных устройств.

2) Усиление политик безопасности, входящих в базовые конфигурации, с акцентом на возможную реализацию угроз безопасности информации со стороны внешнего нарушителя с высоким и средним потенциалом.

Отключение беспроводных соединений

Исключение возможности организации беспроводного соединения обеспечивается следующими настройками:

1) Отключение всех беспроводных интерфейсов, например, 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 драйверов звуковой карты и UVC-устройств, например:

blacklist snd_hda_intel

blacklist uvcvideo

2.4. Конфигурирование наиболее уязвимых системных служб

Конфигурирование SSH

Конфигурирование параметров, отвечающих за безопасность функционирования при подключении к сетям общего доступа, 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
4.	Запретить использование протокола SSH1	Protocol 2

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

№ п/п	Описание настройки	Конфигурируемый параметр
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 соответствующих параметров в соответствующие конфигурационные файлы параметров ядра, например, /etc/sysctl.conf;

– с использованием графический инструмента «Управление политикой безопасности» (fly-admin-smc) по пути «Пуск» - «Панель управления» - «Безопасность» - «Политика безопасности» - «Настройки безопасности» - «Параметры ядра» - «Шаблоны» путем внесения изменений в шаблоны настроек.

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	net.ipv4.ip forward=0
2.	Параметры, отвечающие за выдачу ICMP Redirect (ICMP перенаправления) другим хостам	net.ipv4.conf.all.accept_redirects=0 net.ipv4.conf.all.secure_redirects=0 net.ipv4.conf.all.send_redirects=0
3.	Ограничение небезопасных вариантов работы с жесткими ссылками (hardlinks)	fs.protected_hardlinks = 1
4.	Ограничение небезопасных вариантов прохода по символическим ссылкам (symlinks)	fs.protected_symlinks = 1
5.	Запрет создания core dump для некоторых исполняемых файлов	fs.suid_dumpable=0
6.	Рандомизация адресного пространства, которая защищает от атак на переполнение буфера	kernel.randomize_va_space=2
7.	Использование фильтрации обратного пути по умолчанию	net.ipv4.conf.default.rp_filter=1
8.	Использование фильтрации обратного пути у всех интерфейсов	net.ipv4.conf.all.rp_filter=1
9.	Ограничение доступа к журналу ядра	kernel.dmesg_restrict=1
10.	Запретить подключение к другим процессам с помощью ptrace	kernel.yama.ptrace_scope=3
11.	Инициализация динамической ядерной памяти нулем при ее выделении	init_on_alloc = 1
12.	Рандомизация расположения ядерного стека	randomize_kstack_offset=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.	Отключение технологии Transactional Synchronization Extensions (TSX)	tsx=off
17.	Настройка параметра ядра, определяющего	vm.mmap_min_addr = 65536

№ п/п	Описание настройки	Конфигурируемый параметр
	минимальный виртуальный адрес, который процессу разрешено использовать для mmap. 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) при возникновении нештатных ситуаций, связанных с установкой обновлений программного обеспечения. 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 утилит установки обновлений с возможностью гибкой настройки fly-astra-update и astra-update.

2.7. Рекомендации по резервному копированию

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

Рекомендуется создание полного образа ОС и установленного ПО. Полный образ представляет собой полную резервную копию (full backup) 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, а также после создания всех пользовательских и административных учетных записей пользователей, а также настройки сетевого окружения для обеспечения работы в сети. Первичный образ используется для полного восстановления ОС и приложений в случае сбоя или нестабильности работы

операционной системы.

Рекомендуется создание последующих образов ОС. В течение эксплуатации операционной системы с периодичностью, установленной в плане резервного копирования, должны создаваться последующие образы. В каждый момент времени должно храниться, 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 использовать утилиту командной строки - rsync.

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

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

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 «Средства резервного копирования и восстановления ОС» 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 отнесены 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 с помощью параметра <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 будет.

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 осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Дополнительно» → путем выключения опции «Разрешить вход без пароля»	ИАФ.1
1.2	Запрет автоматического входа в систему по сохраненным учётным данным	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. Настройка осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Дополнительно» → путем выключения опции «Разрешить автоматический вход в систему» - с помощью инструмента astra-autologin-control: astra-autologin-control disable Проверка состояния (значение должно быть enable) astra-autologin-control is-enabled enabled - контроль включен disabled - контроль выключен	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
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 осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Дополнительно» → путем установки для параметра «Автоматически выбирать пользователя» значения «Нет»	ИАФ.1
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 осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Дополнительно» → путем отключения опции «Автоматический вход в систему после сбоя X-сервера»	ИАФ.1
1.5	Запрет использования удаленных сессий	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 осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Дополнительно» путем отключения опции «Разрешить удаленные сессии»	ИАФ.1 УПД.13
1.6	Запрет входа системных учетных записей	С целью реализации мер защиты информации, направленных на обеспечение безопасности оболочки системы и нейтрализацию угроз использования механизмов авторизации для повышения привилегий,	ИАФ.1

№	Наименование настройки	Действия / Параметр	Мера
		рекомендуется запретить графический вход в систему под учётными записями, не связанными с конкретными пользователями в системе. Настройка осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Пользователи» путем установки диапазона значений идентификаторов 1000 - 29999 для параметра «Идентификаторы системных пользователей»	
1.7	Запрет показа списка пользователей на экране входа	С целью реализации мер защиты информации, направленных на защиту аутентификационной информации от несанкционированного ознакомления, требуется обеспечить невозможность автоматического выбора пользователя для входа. Настройка осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Пользователи» путем отключения опции «Показывать список».	ИАФ.1 УПД.11
1.8	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 осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Пользователи» путем отключения опции «Автодополнение».	ИАФ.11 УПД.11
1.9	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.	ИАФ.1 УПД.1

№	Наименование настройки	Действия / Параметр	Мера
		Настройка ограничения графического входа root осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Пользователи» путем отключения опции «Разрешить вход администратору root».	
1.10	Настройка входа локальных пользователей в условиях домена	В случае использования в информационной системе доменной структуры следует настроить политику локального входа. Настройка осуществляется с использованием: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика локального входа». При использовании в системе только локальных пользователей должен быть установлен режим «Разрешено всем». Для доменных компьютеров рекомендуется использовать режим входа «Разрешено администраторам».	ИАФ.1 УПД.1
1.11	Ограничение входа суперпользователя	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. С целью ограничения входа суперпользователя необходимо в графическом инструменте «Управление политикой безопасности» (fly-admin-smc) по пути: «Панель Управления» → «Безопасность» → «Политика безопасности» → «Пользователи» → отобразить системных пользователей → выбрать системного пользователя root → «Блокировка» → активировать опцию: «Удаление пароля и блокировка входа».	ИАФ.1 УПД.1
Настройка параметров политики блокировки учетной записи			
1.12	Количество неуспешных	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется	ИАФ.4 УПД.6

№	Наименование настройки	Действия / Параметр	Мера
	попыток, при превышении которого доступ пользователя в систему будет запрещен	настройка блокировки учетных записей пользователя после установленного количества неудачных попыток вводя пароля. Настройка групповой политики осуществляется с использованием: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Блокировка» (политика блокировки учетной записи: настройка pam_tally) путем: 1) Отключения опции «Индивидуальные настройки» 2) Установки соответствующего значения для параметра «Неуспешных попыток». Применение индивидуальных настроек для каждого пользователя осуществляется с использованием: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Блокировка (политика блокировки учетной записи: настройка pam_tally)» путем: 1) Включения опции "Индивидуальные настройки"; 2) После ее активации для каждого (не системного) пользователя по пути «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Пользователи» → <имя пользователя> → «Блокировка» для параметра «максимальное количество неудачных попыток входа» устанавливается индивидуальное значение. При этом если в индивидуальных настройках блокировки для параметра «Максимальное количество неудачных попыток входа» установлено значение «0», то максимальное количество неудачных попыток входа будет соответствовать значению, установленному в глобальной политике (параметр «Неуспешных попыток»).	
1.13	Использование счетчика неудачных попыток для пользователя с uid=0	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 для учетной записи пользователя с uid=0.	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		Настройка осуществляется с использованием: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Управление политикой безопасности» → «Политики учетной записи» → «Блокировка» (политика блокировки учетной записи: настройка pam_tally) путем отключения опции «Не использовать счетчик для пользователя с uid=0».	
1.14	Установка периода блокировки (запрет на повторную попытку входа в систему на определенное количество секунд после неуспешного входа).	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 запрета на повторную попытку входа в систему на заданное количество секунд после неуспешного входа. Настройка осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Блокировка» (политика блокировки учетной записи: настройка pam_tally) путем установки для параметра «Период блокировки» соответствующего значения.	ИАФ.4 УПД.6.
1.15	Установка периода разблокировки (пользователь будет разблокирован после заданного интервала времени (секунды) при блокировке аккаунта после достижения максимального количества неудач)	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 периода разблокировки. Настройка осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Блокировка» (политика блокировки учетной записи: настройка pam_tally) путем установки для параметра «Период разблокировки» соответствующего значения. По истечению заданного периода пользователь будет разблокирован.	ИАФ.4 УПД 6.
Настройка параметров политики сложности паролей			
1.16	Проверка имени пользователя	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики сложности паролей, в	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		том числе пользователям устанавливается запрет на использование своего имени в качестве пароля. Настройка осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Сложность» путем включения опции «Проверка имени пользователя (только для pam_cracklib)».	
1.17	Проверка GECOS	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Сложность» путем включения опции «Проверка GECOS».	ИАФ.4
1.18	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Сложность» путем включения опции «Применять для пользователя root».	ИАФ.4
1.19	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 осуществляется с помощью: - графического инструмента «Управление политикой	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Сложность» путем установки значения для параметра «Минимальная длина пароля».	
1.20	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. Настройка осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Сложность» путем включения опции «Минимальное количество строчных букв в новом паролей» и установкой соответствующего значения.	ИАФ.4
1.21	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Сложность» путем включения опции «Минимальное количество заглавных букв в новом паролей» и установкой соответствующего значения.	ИАФ.4
1.22	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» →	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		«Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Сложность» путем включения опции «Минимальное количество цифр в новом паролей» и установкой соответствующего значения.	
1.23	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Управление политикой безопасности» → «Политики учетной записи» → «Политика паролей» → «Сложность» путем включения опции «Минимальное количество других символов в новом паролей» и установкой соответствующего значения.	ИАФ.4
Настройка параметров политики истории паролей			
1.24	Минимальное количество измененных символов при создании новых паролей	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 осуществляется путем задания соответствующей конфигурации в файле /etc/pam.d/common-password: в строке «password requisite pam cracklib.so..» необходимо установить соответствующее значение для параметра «difok», например: difok = 2.	ИАФ.4
1.25	Запрет на использование пользователями определенного числа последних использованных паролей (в том числе для root)	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров политики истории паролей, в том числе запрет на повторное использование пользователями последних использованных паролей. Настройка осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» →	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
		«Панель Управления» → «Управление политикой безопасности» → «Политики учетной записи» → «Политика паролей» → «История» путем включения опций: «Поддержка истории паролей», «Применять для root» и «Количество паролей, которые нужно запомнить» - путем задания соответствующей конфигурации в файле /etc/pam.d/common-password. В строке, где указан модуль «…pam_unix.so» следует добавить параметр «remember» и установить для него соответствующее значение. Пример: password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass gost12_512 remember= 4	
Настройка параметров политики срока действия паролей			
1.26	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Срок действия» → путем включения опции «Минимальное количество дней между сменами пароля» и установки соответствующего значения.	ИАФ.4
1.27	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Срок действия» → путем включения опции «Максимальное количество дней между сменами пароля» и установки соответствующего значения.	ИАФ.4

№	Наименование настройки	Действия / Параметр	Мера
1.28	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Политика паролей» → «Срок действия» → путем включения опции «Число дней выдачи предупреждения до смены пароля» и установки соответствующего значения.	ИАФ.4
1.29	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 осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Пользователи» → <выбрать пользователя> → «Срок действия» → путем включения опции «Срок действия учетной записи пользователя» и установки соответствующего значения.	ИАФ.4
Дополнительные настройки			
1.30	Запрос пароля при каждом выполнении команды sudo	По умолчанию не требуется вводить пароль при вызове sudo. Это повышает удобство, но в некоторых случаях может быть небезопасно. Включение режима установки запроса пароля при каждом выполнении команды sudo осуществляется по решению администратора: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Политика консоли и интерпретаторов» путем включения опции «Включить	ИАФ.1

№	Наименование настройки	Действия / Параметр	Мера
		ввод пароля для sudo». - с помощью инструмента командной строки astra-sudo-control: sudo astra-sudo-control enable Проверка состояния: 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. Установка единого срока Настройка срока действия для всех пользователей осуществляется путем настройки политики: - с использованием утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Срок действия» путем включения опции «Срок действия учетной записи пользователя» и установки соответствующего значения. Настройка срока действия для каждого пользователя в отдельности осуществляется путем настройки индивидуальной политики: - с использованием утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Пользователи» → выбрать пользователя → «Срок действия» путем включения опции «Срок действия учетной записи пользователя» и установки соответствующего значения.	УПД.1
2.2	Блокирование учетной записи пользователя за период неиспользования	С целью реализации мер защиты информации, направленных на защиту учетных записей, выполняется настройка параметров блокирования учетной записи пользователя через установленный период неиспользования.	УПД.1 ИАФ.3

№	Наименование настройки	Действия / Параметр	Мера
		Настройка осуществляется с помощью: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Политики учетной записи» → «Блокировка» (политика блокировки учетной записи: настройка pam_tally) путем включения опции «Период неактивности» и установки соответствующего значения.	
Ограничение числа параллельных сеансов			
2.3	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя операционной системы	С целью реализации мер защиты информации, связанных с ограничением числа параллельных сеансов доступа, выполняется настройка, позволяющая администратору устанавливать запрет вторичного входа в систему для пользователей или групп. Настройка выполняется в конфигурационном файле /etc/security/limits.conf. Для запрета вторичного входа в систему для всех пользователей, в конце файла следует добавить строки типа: * hard maxlogins 1 Чтобы ограничить вход пользователям по принадлежности к группе (на примере группы test), запись должна иметь следующий вид: %test hard maxlogins 1	УПД.9
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 осуществляется для каждого пользователя с использованием: - графического инструмента «Оформление Fly» (fly-admin-theme) по пути: "Пуск" - "Панель управления" - "Рабочий стол" - "Оформление Fly" - "Блокировка" путем включения опций «Блокировать экран» и установки для параметра «После бездействия» соответствующего значения интервала времени неактивности, по прошествии которого монитор блокируется. Также включаются опции «После бездействия», «Монитор погашен», «Компьютер в режиме сна»,	УПД.10

№	Наименование настройки	Действия / Параметр	Мера
		«Переключение на другую сессию», «Крышка ноутбука закрыта». Для всех новых пользователей системы: - в файле /usr/share/fly-wm/theme/default.themerc для параметра ScreenSaverDelay следует задать значение соответствующего интервала времени неактивности, по прошествии которого монитор блокируется. Например, для 5 минут: ScreenSaverDelay=300 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 осуществляется для каждого пользователя с помощью: - графического инструмента «Оформление Fly» (fly-admin-theme) по пути: "Пуск" - "Панель управления" - "Рабочий стол" - "Оформление Fly" - "Блокировка" путем установки значений времени задержки между попытками и уровня звукового сигнала для параметра «При неверном пароле».	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 осуществляется для каждого пользователя с помощью: - графического инструмента «Оформление Fly» (fly-admin-theme) по пути: «Пуск» - «Панель управления» - «Рабочий стол» - «Оформление Fly» - «Блокировка» путем включения опций «Переход на другую контроль или сессию» и «Подключение программ из сети».	УПД.10 УПД.11
2.7	Запрет на отображение	С целью реализации мер защиты информации, связанных с защитой пользовательских сессий,	УПД.10

№	Наименование настройки	Действия / Параметр	Мера
	информации сеанса пользователя на экране блокировки	выполняется настройка запрета отображения информация о сеансе пользователя на устройстве отображения (мониторе) после блокировки сеанса доступа пользователя. Настройка осуществляется: - для каждого уже созданного пользователя в файле /home/$пользователь/.fly/theme/current.themerc путем установки для параметра «LockerShowUsername» значения «false»; - для новых создаваемых пользователей в файле /usr/share/fly-wm/theme/default.themerc путем установки для параметра «LockerShowUsername» значения «false».	
2.8	Настройка параметров энергосбережения	С целью реализации мер защиты информации, связанных с защитой конфиденциальной информации от несанкционированного доступа и утечки, по возможности рекомендуется не использовать спящие режимы энергосбережения. Настройка осуществляется для каждого пользователя с использованием: - графического инструмента «Электропитание» (fly-admin-theme) по пути: «Пуск» - «Панель управления» - «Оборудование» - «Электропитание» - «Энергосбережение» путем установки для параметра «При приостановке сеанса» значения «Ничего не делать» и отключения опции «Переходить из сна в гибернация при бездействии». В случае необходимости использования спящих режимов для обеспечения доступности информации в случае нарушения электроснабжения, следует использовать инструмент astra-swapwiper-control, входящий в состав ОС и предназначенный для стирания данных, находящихся в дисковых разделах подкачки, при выключении системы. Для обеспечения надёжной защиты от несанкционированного доступа данных в областях подкачки рекомендуется использовать предусмотренную в ОС возможность автоматического защитного преобразования данных дисков и областей подкачки.	УПД.2 ЗТС.5

№	Наименование настройки	Действия / Параметр	Мера
Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации			
2.9	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 осуществляется с использованием: - инструмента astra-nobootmenu-control: astra-nobootmenu-control enable Проверка состояния (значение должно быть enable) astra-nobootmenu-control is-enabled enabled - контроль включен disabled - контроль выключен	УПД.11 ОПС.1 УПД.17
2.10	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 осуществляется с в конфигурационном файле /etc/default/grub путем добавления параметра GRUB_DISABLE_RECOVERY="true" Для вступления изменений в силу обновить загрузчик командой: sudo update-grub	УПД.11 ОПС.1
2.11	Исключение возможности удаленного выключения и перезагрузки машины непривилегированным пользователям	С целью реализации мер защиты информации, направленных на защиту сетевых соединений, а также на нейтрализацию угроз использования слабостей протоколов сетевого взаимодействия, рекомендуется запретить непривилегированным пользователям возможность удаленного выключения компьютера. Настройка осуществляется с использованием: - графического инструмента «Настройка графического входа» (fly-admin-dm) по пути: «Пуск» → «Панель управления» → «Система» → «Вход в систему» → «Выключение» → «Разрешить выключать компьютер» → для параметра «Удаленно» установить значение «Только администратору».	УПД.11

№	Наименование настройки	Действия / Параметр	Мера
2.12	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 для пользователей. 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 (sudo systemctl ...). Изменение режима блокировки вступает в действие немедленно. Настройка осуществляется по решению администратора: - с использованием графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки» безопасности → «Системные параметры» → «Выключение / перезагрузка ПК» путем включения/отключения опции «Блокировка выключения/ перезагрузки ПК для пользователей» - с помощью инструмента командной строки astra-shutdown-lock: astra-shutdown-lock enable/disable Проверка состояния astra-shutdown-lock is-enabled enabled включен disabled выключен Failed to get unit file state ... сервис не активирован	УПД.11
Настройка дискреционных правил разграничения доступом			
2.13	Контроль дискреционных прав доступа к объектам файловой системы	С целью реализации мер защиты информации, направленных на защиту от несанкционированной подмены атрибутов безопасности субъектов доступа, а также несанкционированного изменения файлов важных системных директорий, рекомендуется осуществлять их контроль. Выполнить проверку параметров прав доступа у файлов, содержащих информацию о локальных учётных записях:	УПД.2

№	Наименование настройки	Действия / Параметр	Мера
		/etc/shadow -rw-r----- (640) Владелец: root Группа: shadow /etc/passwd -rw-r--r-- (644) Владелец: root Группа: root /etc/group -rw-r--r-- (644) Владелец: root Группа: root /etc/crontab -r-------- (400) Владелец: root Группа: root 2) Выполнить проверку прав доступа внутри важных системных каталогов. Данная группа параметров предназначена для настройки прав доступа к важным системным каталогам, к которым отнесены следующие параметры: - проверка прав доступа разделяемых библиотек и модулей: /usr/lib /usr/lib64 /lib /lib64 У директорий внутри каталогов (d): drwxr-xr-x (755) Владелец: root Группа: root У файлов (-): -rw-r--r-- (644) Владелец: root Группа: root /lib/modules/<версия ядра>/ /lib/modules/<версия ядра>/ У директории внутри: drwxr-xr-x (755) Владелец: root Группа: root У файлов (-): -rw-r--r-- (644) Владелец: root Группа: root	

№	Наименование настройки	Действия / Параметр	Мера
		/usr/libexec — У директорий (d) и всех файлов внутри этих директорий: rwxr-xr-x (755) Владелец: root Группа: root - проверка прав доступа системных конфигурационных файлов: /etc/cron.d/anacron, /etc/cron.d/logcheck, /etc/anacrontab, /etc/cron.daily/..., /etc/cron.hourly/..., /etc/cron.weekly/..., /etc/cron.monthly/... — -rw-r--r-- (644) Владелец: root Группа: root; -rwxr-xr-x (755) Владелец: root Группа: root /etc/crontab — -r-------- (400) Владелец: root Группа: root /etc/profile.d/... — У файлов внутри директории: /etc/profile — -rw-r--r-- (644) Владелец: root Группа: root У директории /etc/profile.d: rwxr-xr-x (755) Владелец: root Группа: root umask = 077 /etc/bash.bashrc — -r-r--r-- (444) Владелец: root Группа: root umask = 077 /etc/fstab, /etc/fstab.bak, /etc/fstab.pdac — -rw-r--r-- (644) Владелец: root Группа: root /etc/fstab.d — drwxr-xr-x (755) Владелец: root Группа: root	

№	Наименование настройки	Действия / Параметр	Мера
		/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 Все файлы .conf -rw-r--r-- (644) Владелец: root Группа: root /var/spool/cron/ drwx-wx–T Владелец: root Группа: crontab /usr/sbin/cron /usr/sbin/anacron -rwxr-xr-x (755) Владелец: root Группа: root (umask = 077) /root/.profile /root/.bashrc Владелец: root Группа: root - проверка прав доступа системных исполняемых файлов: /bin /usr/bin /usr/local/bin /sbin /usr/sbin /usr/local/sbin /usr/sbin/service -rwxr-xr-x (755) -rwsr-xr-x (4755) /var/log/audit/audit.log -rwxr-sr-x (2755) Владелец: root Группа: root -rwxr-xr-x (755) Владелец: root Группа: root	

№	Наименование настройки	Действия / Параметр	Мера
		- проверка прав доступа домашних директорий: /home/<имя пользователя> drwx------ (700) Владелец: root Группа: shadow - проверка прав доступа журналов аудита: /var/log/audit drwxr-x--- (750) Владелец: root Группа: adm /var/log/audit/audit.log.1 /var/log/audit/audit.log.2 /var/log/audit/audit.log.3 /var/log/audit/audit.log.4 -r--r----- (440) Владелец: root Группа: adm /var/log/audit/audit.log -rw-r----- (640) Владелец: root Группа: adm Для системных файлов, как правило, должно быть установлено значение umask = 077. Установка этого значения umask означает, что к указанным файлам имеет доступ только суперпользователь root.	
Разграничение доступа к устройствам			
2.14	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: - в графическом режиме с помощью графического инструмента Управление политикой безопасности» (fly-admin-smc) по пути: «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки» безопасности → «Системные параметры» путем включения опции «Запрет монтирования носителей непривилегированным пользователем» - с помощью инструмента командной строки astra-mount-	УПД.15 ЗНИ.5 ЗНИ.6 ЗНИ.7 ЗИС.30

№	Наименование настройки	Действия / Параметр	Мера
		lock: astra-mount-lock enable/disable Проверка состояния astra-mount-lock is-enabled enabled включен disabled выключен Failed to get unit file state ... сервис не активирован После включения режима для того, чтобы непривилегированный пользователь системы мог выполнить полуавтоматическое монтирование носителей информации, необходимо осуществить его обязательную регистрацию в соответствии с положениями раздела «Средства разграничения доступа к подключаемым устройствам» документа «Руководство администратора. Часть 1».	
2.15	Включение режима запрета форматирования съемных машинных носителей информации непривилегированным пользователям	С целью реализации мер защиты, связанных с контролем доступа к мобильных 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 помощью инструмента командной строки astra-format-lock: astra-format-lock enable/disable Проверка состояния astra-format-lock is-enabled enabled включен disabled выключен Failed to get unit file state ... сервис не активирован	УПД.15 ЗНИ.8 ЗИС.30
Ограничение на использование технологий беспроводного доступа			
2.16	Ограничение доступа к Wi-Fi	С целью реализации мер защиты, связанных с ограничением доступа к беспроводным соединениям, выполняется настройка ограничения доступа к Wi-Fi. Предоставление доступа к системам беспроводного	УПД.14 ЗИС.20

№	Наименование настройки	Действия / Параметр	Мера
		доступа должно осуществляться только тем пользователям, кому он необходим для выполнения должностных обязанностей. Ограничение доступа к Wi-Fi (например, только для группы netdev) можно настроить с использованием политики PolicyKit-1. В файле политики /var/lib/polkit-1/localauthority/75-polkitfly.d/org.freedesktop.NetworkManager.pkla задать следующие параметры: [lockwifi] Identity=unix-group:netdev; Action=org.freedesktop.NetworkManager.enable-disable-wifi ResultAny=yes ResultInactive=yes ResultActive=yes [lockwifi] Identity=unix-group:netdev; Action=org.freedesktop.NetworkManager.network-control ResultAny=yes ResultInactive=yes ResultActive=yes [lockwifi] Identity=unix-group:netdev; Action=org.freedesktop.NetworkManager.enable-disable-network ResultAny=yes ResultInactive=yes ResultActive=yes В файле политики /usr/share/polkit-1/actions/org.freedesktop.NetworkManager.policy в секциях: org.freedesktop.NetworkManager.enable-disable-wifi org.freedesktop.NetworkManager.network-control org.freedesktop.NetworkManager.enable-disable-network установить значение «no» в строках: <defaults> <allow_inactive>no</allow_inactive> <allow_active>no</allow_active>	

№	Наименование настройки	Действия / Параметр	Мера
		<allow_any>no</allow_any> </defaults> После выполненных настроек доступ к wifi будет только у пользователей, состоящих в группе netdev.	
2.17	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 Bluetooth выполняется путем редактирования настроек файла /etc/dbus-1/system.d/bluetooth.conf. В нем необходимо удалить строки: /etc/dbus-1/system.d/bluetooth.conf <policy at_concole="true"> <allow send_destination="org.bluez"/> </policy> После выполнения перезагрузки, доступ к устройствам bluetooth будут иметь только пользователи системной группы bluetooth.	УПД.14 ЗИС.20
МКЦ			
2.18	Включение мандатного контроля целостности	В целях реализации мер защиты информации, направленных на исключение скрытых каналов (информационных потоков) при защите от угрозы целостности информации, 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 с использованием: - графического инструмента «Политика безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Мандатный контроль	ЗИС.16 ЗИС.15 ОЦЛ.8 УПД.5 ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		целостности» путем включения опции «Подсистема Мандатного Контроля Целостности», а также режимов «Защита файловой системы», «Запуск сервисов на изолированном уровне» с настройкой параметров в «режиме эксперта»; - с помощью инструмента astra-mic-control: astra-mic-control enable Проверить включился ли режим МКЦ командой: astra-mic-control status Назначение мандатных атрибутов целостности пользователей осуществляется с использованием: - графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Пользователи» → <пользователь> → «МРД» путем установки доступных уровней целостности пользователя. При включении МКЦ для системного параметра ядра в загрузчике ОС Grub устанавливается значение max_ilev=63 — максимальный уровень целостности по умолчанию. Все процессы, начиная от init до утилиты графического входа в систему fly-dm, будут запускаться на данном уровне целостности. Выключение МКЦ крайне не рекомендуется, т.к. многие механизмы защиты связаны с включенным режимом МКЦ, а именно: блокировка интерпретаторов, nochmodx, блокировка доступа с конфиденциальной информации и т.д.	
2.19	Управление запуском сетевых сервисов на пониженном уровне МКЦ	С целью реализации мер защиты информации, направленных на защиту системного программного обеспечения ОС от возможного воздействия сетевых сервисов, 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.	ЗИС.16 ЗИС.15 ОЦЛ.8 УПД.5 ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		Включение режима осуществляется с помощью инструмента командной строки astra-ilev1-control: astra-ilev1-control enable/disable Проверка состояния astra-ilev1-control is-enabled enabled включен disabled выключен	
2.20	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 помощью инструмента командной строки astra-docker-isolation: astra-docker-isolation enable Проверка состояния astra-docker-isolation is-enabled enabled включен disabled выключен	ЗИС.16 ЗИС.15 ОЦЛ.8 УПД.5 ОПС.1
2.21	Управление расширенным режимом мандатного контроля целостности	Расширенный режим МКЦ применяется по решению администратора системы для усиления защиты ОС. В режиме МКЦ процесс при его непосредственном запуске наследует уровень целостности процесса-родителя. При этом в расширенном режиме МКЦ (strict mode) непосредственный запуск процесса запрещен в том случае, если исполняемый файл, из которого запускается процесс, имеет уровень целостности меньше или несравнимый с уровнем целостности процесса-родителя. В данном случае процесс возможно запустить только с использованием инструмента sumic. Вместе с тем его включение может привести к сбоям в работе некоторого прикладного ПО (особенно уже	ЗИС.16 ЗИС.15 ОЦЛ.8 УПД.5 ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		установленного). Поэтому перед включением расширенного режима МКЦ в ОС администратору рекомендуется провести тестирование используемого прикладного ПО с целью проверки его работоспособности при включенном расширенном режиме МКЦ и необходимости его дополнительной настройки. Включение расширенного режима МКЦ осуществляется путем выполнения от имени администратора команды: astra-strictmode-control enable Выключение расширенного режима мандатного контроля целостности (опция disable) не поддерживается. Изменение режима вступает в действие после перезагрузки.	
МРД			
2.22	Включение мандатного управления доступом	По решению администратора об использовании в системе в качестве дополнительной меры мандатного метода управления доступом выполняется его включение и настройка. Включение в системе мандатного управления доступом осуществляется с использованием: - инструмента командной строки astra-mac-control: astra-mac-control enable - графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Мандатное управление доступом» путем включения опции «Подсистема Мандатного Управления Доступом». Настройка уровней конфиденциальности осуществляется с использованием: - графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Мандатные атрибуты» → «Категории» / «Уровни конфиденциальности» путем определения и установкой возможных уровней конфиденциальности в системе.	УПД.12 ЗИС.16 ОЦЛ.6 УПД.2

№	Наименование настройки	Действия / Параметр	Мера
		Назначение мандатных привилегий и мандатных атрибутов пользователей осуществляется с использованием: - графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Пользователи» → <пользователь> → МРД путем установки минимального и максимального уровня конфиденциальности пользователя.	
2.23	Включение режимов AstraMode и MacEnable	Для поддержки работы сервиса apache2 и сервера печати CUPS в условиях мандатного разграничения доступа выполняется их настройка. Настройка осуществляется с использованием: - инструмента командной строки astra-mac-control: astra-mode-apps enable Для применения изменений требуется перезапуск служб. - графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Мандатное управление доступом» путем включения опции «Apache» и «Cups».	УПД.12 ЗИС.16 ОЦЛ.6 УПД.2
2.24	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 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: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Системные параметры» путем включения опции «Блокировка одновременной	УПД.12 ЗИС.16 ОЦЛ.6 УПД.2 УПД.5 ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		работы с разными уровнями Sumac в пределах одной сессии» - с помощью инструмента командной строки astra-sumac-lock: sudo astra-sumac-lock enable/disable Проверка состояния: astra-sumac-lock is-enabled enabled включен disabled выключен Failed to get unit file state ... сервис не активирован	
2.25	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, т.к. с их помощью можно организовать скрытый канал передачи информации между уровнями. Изменение режима блокировки вступает в действие немедленно. Включение режима осуществляется: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Системные параметры» путем включения/отключения опции «Блокировка системных команд для пользователей» - с помощью инструмента командной строки astra-commands-lock: astra-commands-lock enable/disable Проверка состояния astra-commands-lock is-enabled enabled включен	ЗИС.16 ОПС.1 УПД.5

№	Наименование настройки	Действия / Параметр	Мера
		disabled выключен	
2.26	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			
2.27	Управление межсетевым экраном ufw	По решению администратора об использовании встроенных механизмов фильтрации сетевых потоков в качестве дополнительной меры по защите информации выполняется включение встроенного межсетевого экрана. Включение межсетевого экрана ufw осуществляется: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки» безопасности → «Системные параметры» → «Межсетевой экран» путем включения опции «Включение межсетевого экрана» - с помощью инструмента командной строки astra-ufw-control: astra-ufw-control enable Проверка состояния astra-ufw-control is-enabled enabled включен disabled выключен	УПД.3
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. Для реализации мер защиты информации, Ограничение на использование графической утилиты «Менеджер пакетов Synaptic» осуществляется средствами графической утилиты PolicyKit-1 («Пуск» → «Панель Управления» → «Безопасность» → «Санкции	ОПС.3

№	Наименование настройки	Действия / Параметр	Мера
		PolicyKit-1). Для этого в разделах дерева выбрать com.ubuntu → pkexec → synaptic – в каждой группе явной (при наличии) и неявной авторизации должны быть заданы параметры аутентификации только для администраторов (групп администраторов).	
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: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Системные параметры» → путем включения опции «Запрет установки бита исполнения для всех пользователей, включая администратора»; - с помощью инструмента командной строки astra-nochmodx-lock: sudo astra-nochmodx-lock enable Проверка состояния: cat /parsecfs/nochmodx 1 включен 0 выключен	ОПС.1 ОЦЛ.7

№	Наименование настройки	Действия / Параметр	Мера
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: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Системные параметры» → путем включения/отключения опции «Блокировка макросов» - с помощью инструмента командной строки astra-macros-lock: sudo astra-macros-lock enable/disable Проверка состояния: astra-macros-lock is-enabled enabled включен disabled выключен	ОПС.1
3.4	Включение блокировки трассировки ptrace для всех пользователей, включая администраторов	С целью реализации мер защиты информации, связанных с ограничением программной среды и направленных на 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.	ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		Включение режима осуществляется: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Системные параметры» путем включения/отключения опции «Блокировка трассировки ptrace для всех пользователей, включая администраторов». - с помощью инструмента командной строки astra-ptrace-lock: sudo astra-ptrace-lock enable/disable Проверка состояния: 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: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Системные параметры» → путем включения опции «Включение системных ограничений ulimits»; - с помощью инструмента командной строки astra-ulimits-control: astra-ulimits-control enable/disable Проверка состояния astra-ulimits-control is-enabled enabled включен disabled выключен	ЗИС.22 ОДТ.1, ОДТ.3 УПД.9
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	ЗИС.22 ОДТ.1 ОДТ.3

№	Наименование настройки	Действия / Параметр	Мера
		пользователями дисковой памяти и количества файлов, принадлежащих пользователю. Настройка выполняется с использованием: - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Управление квотами» путем: 1) включения опций «Поддержка квот для пользователей» и/или «Поддержка квот для групп»; 2) настройкой оповещений для пользователей и групп о превышении установленных квот; 3) установкой мягкий и жестких ограничений на использование пользователями/группами дисковой памяти и количества файлов по пути: «Политика безопасности» → «Группы» → выбрать группу → «Квоты» для групп и/или «Политика безопасности» → «Пользователи» → выбрать пользователя → «Квоты» для пользователей.	
3.7	Включение загрузки модуля ядра lkrg	С целью реализации мер защиты информации, направленных на защиту пространства памяти ядра от модификации и обнаружения некоторых уязвимостей, возможно применение модуля ядра lkrg, который обеспечивает мониторинг угроз и блокирование несанкционированных изменений в ядре ОС. Инструмент astra-lkrg-control управляет загрузкой модуля ядра lkrg и настраивает его автозагрузку. Включение режима осуществляется с помощью инструмента командной строки astra-lkrg-control: astra-lkrg-control enable Проверка состояния astra-lkrg-control is-enabled enabled включен disabled выключен	ОПС.1 ЗИС.19 ЗИС.21
3.8	Включение блокировки неиспользуемых модулей ядра	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на минимизацию количества включенного в состав ОС компонент, что позволит существенно уменьшить перечень потенциально уязвимых компонентов, тем самым сократив поверхность атаки, выполняется включение режима блокировки неиспользуемых модулей	ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		ядра. Неиспользуемыми считаются те модули, которые не загружены в момент включения astra-modban-lock. Включение блокировки загрузки неиспользуемых модулей ядра осуществляется с помощью инструмента командной строки astra-modban-lock: astra-modban-lock enable/disable Проверка состояния astra-modban-lock is-enabled enabled включен disabled выключен	
3.9	Включение блокировки автоматического конфигурирования сетевых подключений	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на ограничение действий пользователей по возможностям управления сетевыми средствами, 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 помощью инструмента командной строки astra-noautonet-control: astra-noautonet-control enable Проверка состояния astra-noautonet-control is-enabled enabled включен disabled выключен	ОПС.1
3.10	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, т.к. их использование пользователем может быть небезопасно. Для этого изменяется значение параметра kernel.sysrq. Значение параметра сохраняется в файл /etc/sysctl.d/999-	ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
		astra.conf. По умолчанию эта функция безопасности включена, т.е. клавиша SysRq не работает. Ограничение работы функций системы, доступных при нажатии клавиши SysRq, осуществляется: - в графическом режиме с помощью графического инструмента Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Системные параметры» → «Клавиши SysRq» путем включения/отключения опции «Блокировка клавиш SysRq для всех пользователей, включая администраторов» - с помощью инструмента командной строки: sysctl -w kernel.sysrq=1 Проверка состояния cat /proc/sys/kernel/sysrq 0 включен 1 выключен	
3.11	Управление блокировкой загрузкой ядра hardened	Инструмент astra-hardened-control включает/отключает в загрузчике GRUB 2 загрузку ядра hardened по умолчанию, если оно присутствует в системе. Ядро с усиленной самозащитой Hardened предоставляет дополнительные возможности по очистке остаточной информации: очистку остаточной информации в ядерном стеке (STACKLEAK), очистку остаточной информации в ядерной куче (PAGE_POISONING). Включение/отключение режима осуществляется по решению администратора с помощью инструмента командной строки astra-hardened-control: astra-hardened-control enable/disable Проверка состояния astra-hardened-control is-enabled enabled включен disabled выключен	Косвенно ОПС.1
3.12	Управление режимом работы файловой системы ОС -	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	ЗИС.18

№	Наименование настройки	Действия / Параметр	Мера
	«только чтение»	системы ОС - «только чтение». Инструмент astra-overlay включает overlay на корневой файловой системе (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. Эта функция может применяться в тех случаях, когда носитель, на котором расположена корневая ФС, аппаратно защищен от записи, либо необходимо программно защитить ее от изменений. Функционал overlay не касается файловых систем, хранящихся на отдельных разделах, отличных от 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: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки» безопасности → «Системные параметры» путем включения/отключения опции «Включить режим работы файловой системы ОС → «только чтение».	

№	Наименование настройки	Действия / Параметр	Мера
		- с помощью инструмента командной строки astra-overlay: astra-overlay enable/disable Проверка состояния astra-overlay is-enabled enabled включен disabled выключен	
3.13	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 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: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Политика консоли и интерпретаторов» → «Консоль» путем включения/отключения опции «Включить блокировку консоли для пользователей не входящих в группу astra-console». - с помощью инструмента командной строки astra-console-lock sudo astra-console-lock enable Проверка состояния: astra-console-lock is-enabled enabled включен disabled выключен	ОПС.1

№	Наименование настройки	Действия / Параметр	Мера
3.14	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). Блокировка осуществляется: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Политика консоли и интерпретаторов» путем включения опции «Включить блокировку интерпретаторов кроме Bash для пользователей». - с помощью инструмента командной строки astra-interpreters-lock: sudo astra-interpreters-lock enable Проверка состояния astra-interpreters-lock is-enabled enabled включен disabled выключен	ОПС.1 ОЦЛ.1 ЗИС.7 ЗИС.22
3.15	Блокировка интерпретатора Bash	Блокировка интерпретатора Bash аналогична блокировке других интерпретаторов команд, вынесена в отдельную блокировку, т.к. 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: - в графическом режиме с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель Управления» →	ОПС.1 ОЦЛ.1 ЗИС.7 ЗИС.22

№	Наименование настройки	Действия / Параметр	Мера
		«Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Политика консоли и интерпретаторов» путем включения опции «Включить блокировку интерпретатора Bash для пользователей». - с помощью инструмента командной строки astra-bash-lock: sudo astra-bash-lock enable/disable Проверка состояния: astra-bash-lock is-enabled enabled включен disabled выключен	
Настройка киоска			
3.16	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. Режим графического киоска настраивается для каждого пользователя с помощью графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Пользователи» → выбрать пользователя → «Графический киоск Fly» → путем включения опции «Режим графического киоска Fly». Флаг включает 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.	ОПС.1 (усиление 1) ОЦЛ.6 ЗИС.1

№	Наименование настройки	Действия / Параметр	Мера
		устанавливаются в соответствии с предоставленным доступом. Настройка глобальных параметров киоска осуществляется: - с использованием графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Глобальные настройки киоска».	
3.17	Применение системного киоска	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на ограничения 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» → «Панель управления» → «Безопасность» → «Системный киоск». Инструмент позволяет включать и отключать режим киоска через графическое меню "Правка" - "Включить режим киоска" или кнопкой с изображением ключей в панели кнопок. Кроме того, инструмент позволяет: изменять содержимое файлов профилей (на снимке экрана приведено содержимое стандартного профиля fly-desktop, включающего стандартный профиль fly-unlock); создавать и изменять профили пользователей.	ОПС.1 ОЦЛ.6 ЗИС.1 ЗИС.22
Настройка ЗПС			
3.18	Включение механизма	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на	ОПС.1 ОЦЛ.1

№	Наименование настройки	Действия / Параметр	Мера
	контроля целостности исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение	обеспечение динамического контроля целостности запускаемых компонентов 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", пункт «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 ЭЦП 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 «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Замкнутая программная среда» → «Настройки» → «Панель управления» → «Контроль исполняемых файлов» → «Включить». На предложение перезагрузки ответить положительно. - путем редактирования файла /etc/digsig/digsig_initramfs.conf – параметра DIGSIG_ELF_MODE установить значение 1: DIGSIG_ELF_MODE=1 После внесения изменений в конфигурационный файл /etc/digsig/digsig_initramfs.conf и необходимо выполнить: sudo update-initramfs -u -k all - с использованием инструмента командной строки astra-digsig-control: sudo astra-digsig-control enable Проверка состояния: astra-digsig-control is-enabled enabled включен disabled выключен	ИАФ.7 ЗИС.7 ЗИС.15 ЗИС.18 ЗИС.22
3.19	Включение механизма контроля целостности	С целью реализации мер защиты, связанных с ограничением программной среды и направленных на обеспечение динамического контроля целостности не подлежащих изменению файлов, в том числе	ОПС.2 АНЗ.3 ОПС.1 ИАФ.7

№	Наименование настройки	Действия / Параметр	Мера
	файлов при их открытии на основе ЭП в расширенных атрибутах файловой системы	поставленных на контроль параметров настройки программного обеспечения и средств защиты информации, выполняется включение механизма контроля целостности файлов при их открытии на основе ЭП в расширенных атрибутах файловой системы. Включение механизма проверки подписей в режиме запрета открытия поставленных на контроль файлов с неверной ЭЦП или без ЭЦП в расширенных атрибутах файловой системы осуществляется: - с использованием графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Замкнутая программная среда» → «Настройки» → «Панель управления» → «Контроль исполняемых файлов» → «Включить». 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 и необходимо выполнить: sudo update-initramfs -u -k all Для контроля файлов необходимо настроить шаблоны имен, используемых при проверке ЭЦП в расширенных атрибутах ФС: - в файле /etc/digsig/xattr_control задать их список. Каждая строка задает свой шаблон в виде маски полного пути. - с использованием графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Замкнутая программная среда» → «Настройки» → задать перечень подвергаемых контролю файлов. После внесения изменений в конфигурационный файл /etc/digsig/digsig_initramfs.conf необходимо от имени учетной записи администратора выполнить команду: sudo update-initramfs -u -k all	ЗИС.15
4	**Защита памяти**		
4.1	Включение	С целью реализации мер защиты, связанных очисткой	ЗИС.21

№	Наименование настройки	Действия / Параметр	Мера
	механизма очистки памяти	освобождаемой памяти (остаточной информации) и направленных 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 снижает скорость выполнения операций удаления и усечения размера файла. Механизм очистки памяти активируется параметром secdelrnd в конфигурационном файле /etc/fstab для раздела ФС, 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 «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Политика очистки памяти» → «Гарантированное удаление файлов и папок» путем настройки параметров очистки для установленных в системе устройств и включения опции «Очистка разделов подкачки». - 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: sudo astra-secdel-control enable Проверка состояния: astra-secdel-control is-enabled enabled включен disabled выключен Примечание:	ЗНИ.4 ЗНИ.8 ОПС.4 ЗИС.16

№	Наименование настройки	Действия / Параметр	Мера
		Операции перезаписи для удаления конфиденциальной информации (гарантированное удаление данных файловых объектов в ОС с помощью многократной перезаписи (опции монтирования secdel и secdelrnd)) при применении на SSD-накопителях технически не может гарантировать полное удаление конфиденциальной информации, ранее записанной на SSD-накопитель.	
4.2	Включение механизма очистки разделов подкачки	С целью реализации мер защиты, связанных очисткой освобождаемой памяти и направленных исключение несанкционированного доступа к защищаемой информации, применяется механизм очистки разделов подкачки. Включение очистки разделов подкачки осуществляется - с использованием графической утилиты «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Политика безопасности» → «Настройки безопасности» → «Политика очистки памяти» путем включения опции «Очистка разделов подкачки»; - с использованием утилиты astra-swapwiper-control: sudo astra-swapwiper-control enable Проверка состояния: astra-swapwiper-control is-enabled enabled включен disabled выключен - установкой в конфигурационном файле */etc/parsec/swap_wiper.conf* для параметра ENABLED значения Y.	ЗИС.21 ОПС.4 ЗИС.16
5	**Регистрация событий безопасности**		
	Управление аудитом		
5.1	Включение подсистемы аудита	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности, выполняется включение регистрации событий аудита. Включение подсистемы аудита осуществляется: - с использованием графической утилиты «Конфигурация аудита» (system-config-audit) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Конфигурация аудита» → «Текущий статус» → <Включить>.	РСБ.3
5.2	Включение служб	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о	

№	Наименование настройки	Действия / Параметр	Мера
	логирования syslog-ng и auditd	событиях безопасности, выполняется запуск службы логирования syslog-ng и auditd. Включение службы логирования syslog-ng осуществляется: - с использованием графической утилиты «Настройка регистрации системных событий» по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» → путем включения опции <Запуск службы логирования>. - с использованием консольной утилиты systemctl применением команды: sudo systemctl start syslog-ng Включение службы логирования auditd осуществляется: - с использованием консольной утилиты systemctl применением команды: sudo systemctl start auditd sudo systemctl enable auditd	
Настройка ротации журналов			
5.3	Настройка ротации /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. По умолчанию действие при достижении максимального размера журналов, происходит ротация лог-файлов. Настройка действия производится с использованием графической утилиты «Конфигурация аудита» (system-config-audit) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Конфигурация аудита» → «Конфигурация» → «Настройки» → <Изменить> → «Файл журнала» путем включения опции: - «Сохранить события аудита в файл» - «Принудительно записывать каждые <1> записи» - «Когда размер журнала увеличится до <8> Мб» → - «Чередовать файлы журналов» → - «Сохранять только новые <5> файлы»	РСБ.3
5.4	Настройка ротации /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	РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		ротации журнала событий безопасности /parsec/log/astra/events. Настройка осуществляется с помощью: - графического инструмента "Настройка регистрации системных событий - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» → «Настройки» → «Ротация основного лога» - путем активации опций: - «Количество файлов» и установки соответствующего значения; - «Максимальный размер файла» или «Период ротации» и установки соответствующих значений.	
5.5	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 пакетов, которым требуется ротация.	РСБ.3
5.6	Настройка 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
5.7	Настройка действия admin_space_left при	С целью реализации мер защиты, связанных с осуществлением сбора, записи и хранения информации о событиях безопасности, выполняется настройка выдачи предупреждения администратору при заполнении	РСБ.4

№	Наименование настройки	Действия / Параметр	Мера
	недостаточном месте на диске	установленной оператором части (процента или фактического значения) объема памяти для хранения информации о событиях безопасности. Настройка оповещения производится с использованием графической утилиты system-config-audit («Конфигурация аудита») по пути: «Пуск» → «Панель управления» → «Безопасность» → «Конфигурация аудита» → «Конфигурация» → «Настройки» → <Изменить> → «Мало дискового пространства» путём установки значений для параметров: - «Первый порог» и выбором необходимой реакции; - «Второй порог»: и выбором необходимой реакции.	
Настройка регистрации событий			
5.8	Регистрация событий входа/выхода субъектов доступа и загрузки (останова) ОС	Должна осуществляться регистрация событий входа/выхода субъектов доступа и загрузки (останова) ОС. Настройка регистрации осуществляется с использованием: - графического инструмента "Настройка регистрации системных событий - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Информация о предыдущих входах» - «Успешный вход в систему» - «Выход из системы» - «Неуспешная авторизация» - «Система загружена» - «Система выключена» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 РСБ.3 ОЦЛ.8 УПД.8
5.9	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 - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления»	РСБ.2 РСБ.3 ОЦЛ.8

№	Наименование настройки	Действия / Параметр	Мера
		→ «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Запуск приложения или процесса» - «Завершение приложения или процесса» Регистрация будет осуществляться в журнал /parsec/log/astra/events. - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Управление политикой безопасности» → «Аудит» путем активации опций успеха/отказа для событий: - «exec» или путем задания индивидуальной политики: «Пользователи» → выбрать пользователя → «Аудит» путем активации регистрации соответствующих событий. Регистрация будет осуществляться в журнал /var/log/audit/audit.log	
5.10	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 - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации групп событий: - «События аудита» - «События самодиагностики подсистемы регистрации событий» - «Управление журналами (записями) регистрации событий безопасности» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 РСБ.3 АН3.3 АН3.5
5.11	Регистрация событий по использованию полномочий пользователя	Должна осуществляться регистрация событий по использованию полномочий пользователя. Настройка регистрации осуществляется путем задания глобальной политики с использованием:	РСБ.1 РСБ.3 АН3.5

№	Наименование настройки	Действия / Параметр	Мера
		- графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Управление политикой безопасности» → «Аудит» путем активации опций успеха/отказа для событий: - «mac» - «acl» - «chown» - «chmod» - «cap» - «audit» - «gid» - «uid» - «module» - «mount» - «chroot» - «net» или путем задания индивидуальной политики: «Пользователи» → выбрать пользователя → «Аудит» путем активации регистрации соответствующих событий. Регистрация будет осуществляться в журнал /var/log/audit/audit.log	
5.12	Регистрация по использованию полномочий по изменению 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 - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Вызов chown» - «Вызов chmod» - «Изменение ACL» - «Вызов umask» Регистрация будет осуществляться в журнал /parsec/log/astra/events. - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» →	РСБ.1 РСБ.3 АН3.5

№	Наименование настройки	Действия / Параметр	Мера
		«Панель управления» → «Безопасность» → «Управление политикой безопасности» → «Аудит» путем активации опций успеха/отказа для событий: - «acl» - «chown» - «chmod» или путем задания индивидуальной политики: «Пользователи» → выбрать пользователя → «Аудит» путем активации регистрации соответствующих событий. Регистрация будет осуществляться в журнал /var/log/audit/audit.log	
5.13	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 - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Удаление файла» - «Изменение файла» - «Открытие файла» - «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. - консольного средства setfaud: sudo setfaud -s o:oxudny:oxudny <путь к объекту>. Регистрация будет осуществляться в журнал /var/log/audit/audit.log.	РСБ.1 АНЗ.3 ОЦЛ.8
5.14	Регистрация изменения параметров и настроек системного ПО	Должна осуществляться регистрация изменения параметров и настроек системного программного обеспечения. Настройка регистрации осуществляется с использованием:	РСБ.1 АНЗ.3 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		- графического инструмента "Настройка регистрации системных событий - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Конфигурация компонента программного обеспечения изменена» - группы событий «Установка, изменение системного времени» А также: - «Изменение файла» - «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. - консольного средства setfaud. Для установки регистрации изменения параметров системных настроек, например, в папке /etc/aliases, следует воспользоваться командой: sudo setfaud -m o:y:y /etc/aliases Регистрация будет осуществляться в журнал /var/log/audit/audit.log.	
5.15	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 - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации группы событий: - «Изменение параметров настроек средств защиты информации» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 АНЗ.3 РСБ.3
5.16	Регистрация подключения и	Должна осуществляться регистрация подключения внешних устройств, в том числе через шину USB	РСБ.1 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
	отключения внешних устройств, в том числе через шину USB	Настройка регистрации осуществляется с использованием: - графического инструмента "Настройка регистрации системных событий - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Устройство подключено» - «Обнаружено устройство хранения данных USB» - «Смонтирован машинный носитель информации» - «Устройство отключено» - «Размонтирован машинный носитель информации» Регистрация будет осуществляться в журнал /parsec/log/astra/events. - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Управление политикой безопасности» → «Аудит» путем активации опций успеха/отказа для событий: - «mount» или путем задания индивидуальной политики: «Пользователи» → выбрать пользователя → «Аудит» путем активации регистрации соответствующих событий. Регистрация будет осуществляться в журнал /var/log/audit/audit.log	
5.17	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 - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации	РСБ.1 РСБ.2 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		системных событий» путем включения регистрации событий: - «Запуск приложения или процесса от имени суперпользователя» 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 при необходимости осуществляется в файле конфигурации /etc/snoopy.ini	
5.18	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 - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Начато удаление программного пакета» - «Программный пакет удален или не был установлен» - «Программный пакет установлен или обновлен» - «Начато обновление программного пакета» - «Начата установка программного пакета» - «Устройство подключено» - «Обнаружено устройство хранения данных USB» - «Смонтирован машинный носитель информации» - «Устройство отключено» - «Размонтирован машинный носитель информации» Регистрация будет осуществляться в журнал /parsec/log/astra/events. Для вывода списка оборудования и информации об устройствах рекомендуется инсталлировать утилиту:	РСБ.1 РСБ.3 АН3.4

№	Наименование настройки	Действия / Параметр	Мера
		sudo apt install lshw Проверить аппаратную конфигурацию СВТ можно с помощью команды: sudo lshw	
5.19	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 - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации для группы событий: - «События управления учетными записями пользователей» - «События управления группами пользователей» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.3 РСБ.1
5.20	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 - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации для группы событий: - «Изменение в сетевой адресации» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	АНЗ.3
5.21	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 - Модуль настройки системы" (fly-	ОДТ.1

№	Наименование настройки	Действия / Параметр	Мера
		admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации для группы событий: - «События ресурсов системы» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.22	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 - Модуль настройки системы" (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Удаление файла» (с указанием в параметрах для поиска событий) - «Журнал аудита удалён» - «Журнал событий удалён» Регистрация будет осуществляться в журнал /parsec/log/astra/events. - графического инструмента «Управление политикой безопасности» (fly-admin-smc) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Управление политикой безопасности» → «Аудит» путем активации опций успеха/отказа для событий: - «delete» или путем задания индивидуальной политики: «Пользователи» → выбрать пользователя → «Аудит» путем активации регистрации соответствующих событий. Регистрация будет осуществляться в журнал /var/log/audit/audit.log	РСБ.1 РСБ.3
5.23	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	РСБ.1 АН3.4 РСБ.3

№	Наименование настройки	Действия / Параметр	Мера
		системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Загрузка или выгрузка модуля ядра» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.24	Регистрация блокирования пользователя	Должна осуществляться регистрация событий блокирования пользователя. Настройка регистрации осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Учетная запись заблокирована по истечении количества попыток ввода пароля» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 РСБ.3 АН3.5
5.25	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 - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Изменение наименования учетной записи» - «Смена пользовательского пароля» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 РСБ.3 АН3.5

№	Наименование настройки	Действия / Параметр	Мера
5.26	Регистрация 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 в журнале /var/log/audit/audit.log событий печати осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации групп событий: - «Вывод информации на печать, в том числе защищенной» - «Пользовательские события» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 РСБ.3 ОЦЛ.5
5.27	Регистрация нарушения целостности контролируемых исполняемых модулей и файлов данных	В ОС должна осуществляться регистрация нарушения целостности контролируемых исполняемых модулей и файлов данных с параметрами настройки программного обеспечения и средств защиты информации. Настройка регистрации в журнале /var/log/audit/audit.log событий печати осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Загрузка неподписанного файла заблокирована СЗ ОС (DIGSIG)» Регистрация будет осуществляться в журнал /parsec/log/astra/events. Аудит событий постановки/снятия с контроля целостности исполняемых модулей и файлов данных, а также событий неудачного запуска неподписанных файлов осуществляется в системном журнале /var/log/kern.log и ksystemlog. Журнал/var/log/afick.log отображает события изменения	РСБ.1 РСБ.3 АНЗ.3

№	Наименование настройки	Действия / Параметр	Мера
		подвергаемых контролю с использованием средства afick файлов в системе.	
5.28	Регистрация попыток удаленного доступа	В ОС по умолчанию осуществляется регистрация попыток удаленного доступа в журнале /var/log/auth.log. Настройка регистрации в журнале /var/log/audit/audit.log событий удаленного доступа осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации событий: - «Установка сетевого соединения» - «Сетевое соединение установлено» - «Установлено соединение с Интернетом» - «Неуспешная авторизация» - «Успешный вход в систему» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	РСБ.1 РСБ.3
5.29	Регистрация событий, связанных с доступом субъектов доступа к компонентам виртуальной инфраструктуры	Настройка регистрации в журнале /parsec/log/astra/events событий, связанных с доступом субъектов доступа к компонентам виртуальной инфраструктуры, осуществляется с использованием (предварительно необходима установка пакета astra-kvm-secure): - графического инструмента «Настройка регистрации системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации группы событий: - «Доступ пользователей средства виртуализации к ВМ» - «Управление контрольными точками ВМ» - «Изменение состояние виртуальных машин» - «Управление запуском/остановкой компонент средства виртуализации» - «Управление виртуальными машинами» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	ЗСВ.3
5.30	Регистрация событий,	Настройка регистрации в журнале /parsec/log/astra/events событий, связанных с изменением в составе и	ЗСВ.3

№	Наименование настройки	Действия / Параметр	Мера
	связанных с изменением в составе и конфигурации компонентов виртуальной инфраструктуры	конфигурации компонентов виртуальной инфраструктуры, осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации групп событий: - «Изменение конфигурации средства виртуализации» - «Изменение конфигурации виртуального коммутатора» - «Изменение конфигураций виртуальных машин» - «Изменение конфигурации дискового хранилища» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	
5.31	Регистрация событий, связанных с изменением правил разграничения доступа к компонентам виртуальной инфраструктуры	Настройка регистрации в журнале /parsec/log/astra/events событий, связанных с изменением правил разграничения доступа к компонентам виртуальной инфраструктуры, осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации групп событий: - «Управление атрибутами доступа» - «Изменение ролевой модели» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	ЗСВ.3
5.32	Регистрация событий, связанных с перемещением и размещением виртуальных машин	Настройка регистрации в журнале /parsec/log/astra/events событий, связанных с перемещением и размещением виртуальных машин, осуществляется с использованием: - графического инструмента «Настройка регистрации системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения регистрации группы событий: - «Перемещение виртуальных машин» Регистрация будет осуществляться в журнал /parsec/log/astra/events.	ЗСВ.3
Настройка оповещений			
5.33	Включение	В системе должна быть установлена программа «Центр	УПД.1

№	Наименование настройки	Действия / Параметр	Мера
	оповещений событий безопасности	уведомлений»: # 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 системных событий - Модуль настройки системы» (fly-admin-events) по пути: «Пуск» → «Панель управления» → «Безопасность» → «Настройка регистрации системных событий» путем включения отправки уведомлений (правой кнопкой машины нажать в сроке события и в контекстном меню выбрать «Включить отправку уведомлений») 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»	УПД.8 АНЗ.3 ОДТ.1 РСБ.3
Настройка централизованного сбора журналов			

№	Наименование настройки	Действия / Параметр	Мера
5.34	Использование средств централизованного протоколирования zabbix	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, 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	РСБ.3 РСБ.4 РСБ.5 РСБ.7 РСБ.8 ОДТ.1 ОДТ.3 ОЦЛ.8 УПД.9 АНЗ.4. АНЗ.5 ЗИС.7 ЗСВ.3 ЗСВ.4
Настройка синхронизации времени			
5.35	Настройка синхронизации времени	Должна осуществляться синхронизация системного времени. Для этого необходимо осуществить настройку синхронизации времени в соответствии положениями документа «Руководство администратора. Часть 1» п. «Службы точного времени», в том числе - необходимо определить источник надежных меток времени; - необходимо настроить определенную администратором периодичность синхронизации системного времени с источником надежных меток времени. Настройка осуществляется с использованием: - графического инструмента «Синхронизация времени» (fly-admin-time) по пути: «Пуск» → «Панель управления» → «Система» → «Синхронизация времени» путем активации работы выбранной службы синхронизации, выбором сервера синхронизации и установкой интервала синхронизации в расширенных настройках.	РСБ.6 РСБ.6
6	**Обеспечение целостности**		
Тестирование СЗИ			
6.1	Тестирование СЗИ	В установленный период администратором проводится 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.	ОЦЛ.1 АНЗ.3

№	Наименование настройки	Действия / Параметр	Мера
		Данный набор обеспечивает тестирование всех функций СЗИ от НСД из состава ОС, включая: - управление доступом, - регистрация событий, - очистка памяти, - изоляция модулей, - идентификация и аутентификация. В состав ОС входят средства тестирования функций СЗИ СУБД, обеспечивающие тестирование всех функций СЗИ СУБД, включая управление доступом, регистрацию событий, идентификацию и аутентификацию: - Модуль тестирования механизма дискреционного управления доступом к объектам ФС wx.sh и acl.sh - Модуль тестирования механизма мандатного управления доступом к объектам ФС fmac - Модуль тестирования механизма дискреционного управления доступом к объектам IPC ipc_dac - Модуль тестирования механизма мандатного управления доступом к объектам IPC pc_mac - Модуль тестирования механизма мандатного управления доступом при сетевых взаимодействиях tcpip_mac - Модуль тестирования механизмов работы с памятью и изоляции процессов mem_test - Модуль тестирования механизма очистки памяти внешних носителей secdelrm.sh - Модуль тестирования механизма привилегий процесса cap_mac - Модуль тестирования подсистемы регистрации событий audit_file.sh и audit_proc.sh - СУБД PostgreSQL пакет postgresql-se-test-x.x. Перед проведением тестирования информационная (автоматизированная) 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.	

№	Наименование настройки	Действия / Параметр	Мера
		Тестирование проводится в соответствии с документом «Руководство по КСЗ. Часть 2»	
Регламентный контроль целостности			
6.2	Настройка контроля целостности с использованием средства Afick	Регламентный контроль проверяет целостность и неизменность ключевых для системы файлов, сравнивая их контрольные суммы с эталонными значениями. На контроль целостности должны быть поставлены подлежащие защите исполняемые модули и файлы данных: - критически важные бинарные и конфигурационные файлы операционной системы и прикладного ПО; - файлы образа ядра и загрузчика ОС; - программного обеспечения средств защиты информации, включая их обновления. - архивные файлы, параметры настройки средств защиты информации и программного обеспечения и иные данные, не подлежащие изменению в процессе обработки информации; - перечень (список) компонентов программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники. В конфигурационный файл /etc/afick.conf внести сведения об исполняемых модулях и файлах данных в соответствии с положениями документа «Руководство по КСЗ. Часть 1», п. «Применение регламентного контроля целостности AFICK». После внесение изменений в конфигурационный файл создать базу контрольных сумм и атрибутов при помощи команды: afick -i При запуске AFICK автоматически произведет инициализацию пакетов самотестирования и установит ежедневное задание для CRON. В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после	АН3.3 АН3.4 ОЦЛ.1 ОЦЛ.2 ЗИС.15 ЗИС.18 ОПС.2

№	Наименование настройки	Действия / Параметр	Мера
		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.