**ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО**

*Кафедра № 27 Математического и программного обеспечения*

**УТВЕРЖДАЮ**

Начальник 27 кафедры

полковник С. Войцеховский

(воинское звание, подпись, инициал имени, фамилия)

«___» _____ 2022 г.

Автор: доцент 24 кафедры к.т.н. подполковник С. Краснов

(должность, ученая степень, ученое и воинское звание, инициал имени, фамилия)

Задание на практическое занятие № 2

Тема: «Мандатный контроль целостности»

(наименование темы семинара, лабораторной работы, практического занятия и других видов учебных занятий по тематическому плану изучения дисциплины)

***Обсуждено и одобрено на заседании кафедры***

(предметно-методической комиссии)

«____» _____ 20__ г.

**протокол № _____**

Санкт-Петербург

2022

Перечень заданий:

Обучающийся должен на практическом занятии выполнить индивидуальное задание определенное преподавателем из списка индивидуальных заданий.

**Цель работы:** освоить администрирование основных параметров мандатного контроля целостности в ОССН с применением графических утилит и консольных команд

**Материально-техническое обеспечение:** ОС Astra Linux Special Edition 1.6 (Версия Смоленск, пользователь leti пароль 11111111) с установленным оперативным обновлением 20211126SE16.iso (оперативное обновление №10).

В ОССН наряду с традиционной для ОС семейства Linux системой дискреционного управления доступом реализована система мандатного управления доступом и мандатного контроля целостности на основе МРОСЛ ДП-модели. С этим связано наличие у сущностей ОССН (файлов, каталогов) мандатных меток конфиденциальности и целостности.

Параметрами мандатного управления доступом (мандатной меткой) являются следующие элементы:

уровень доступа или конфиденциальности (соответствует уровню конфиденциальности сущности или доступа субъект-сессии);

набор неиерархических категорий сущности и субъект-сессии;

уровень целостности сущности и субъект-сессии;

специальные атрибуты сущности (CCNR, CCNRI, E_Hole, W_Hole).

При установке ОССН (по умолчанию) задаются следующие параметры мандатного управления доступом и мандатного контроля целостности:

непосредственно используемых уровня целостности («Низкий» значение 0, «Высокий» – 63);

Для выполнения работы необходима установленная ОССН версии 1.6, в которой создана учётная запись пользователя user (учетная запись создается индивидуально по фамилии обучающегося латиницей), с параметрами: максимальный и минимальный уровни доступа – 0, неиерархические категории – нет, уровень целостности – «Высокий», входит в группу администраторов – astra-admin (вторичная группа), разрешено выполнение привилегированных команд (sudo).

Начать работу со входа в ОССН в графическом режиме с учётной записью пользователя user (уровень доступа – 0, неиерархические категории – нет, уровень целостности – «Высокий»).

## Краткие теоретические сведения

Для мандатного контроля целостности используется сценарий pdp-init-fs.

В ОС СН Astra Linux Smolensk Edition 1.6 с установленным обновлением не ниже 20190912SE16 подсистема мандатного контроля целостности включена по умолчанию (иначе отключен), защита файловой системы по умолчанию отключена.

Выключать мандатный контроль целостности не рекомендуется. Например, есть возможность блокировать командные интерпретаторы. При этом, можно настроить их блокировку, но работать она не будет. Блокировка доступа к конфиденциальной информации тоже работать не будет.

Мандатный контроль целостности рекомендуется включать только после того, как вы завершили все настройки безопасности в системе, поскольку все дальнейшее администрирование системы будет доступно только при входе в систему под высоким уровнем целостности.

Фактически, уровень целостности представляет собой маску, которая состоит из единичных битов (рис.1). В ОС СН Astra Linux Smolensk Edition 1.6 по умолчанию работает 7 уровней целостности, которые можно в дальнейшем расширить до 8. Уровни не сравнимые (неиерархические) между собой, это означает что нет вышестоящих или низлежащих уровней целостности. На рис. Приведены уровни целостности и их маски (обратите внимание, что в таблице отсутствует высокий уровень целостности с числом 063). Есть свободные уровни целостности, которые могут быть использованы нами для чего либо, и есть зарезервированные, которые могут быть использованы для настройки максимального уровня целостности. Чаще всего используются два уровня целостности 0 и 63, остальные могут быть актуальными для разработчиков. Значение высокого уровня целостности получается битовой маской с шестью уровнями целостностями. Максимальное значение может быть 255 если используются все уровни целостности. Для ежедневных задач мы используем уровень целостности 0, и только для нужд администрирования – 63.

| № п/п | Значение | Битовая маска | Комментарий |
|---|---|---|---|
| | 000 | 0000 0000 | Нулевой уровень. "Низкий", или "Low" |
| 1 | 001 | 0000 0001 | Уровень задействован как "Сетевые сервисы" |
| 2 | 002 | 0000 0010 | Уровень задействован как "Виртуализация" |
| 3 | 004 | 0000 0100 | Уровень задействован как "Специальное ПО" |
| 4 | 008 | 0000 1000 | Уровень задействован как "Графический сервер" |
| 5 | 016 | 0001 0000 | Свободен, может быть использован для СУБД |
| 6 | 032 | 0010 0000 | Свободен, может быть использован для сетевых сервисов |
| 7 | 064 | 0100 0000 | Зарезервирован, и может быть использован при поднятии max_ilev |
| 8 | 128 | 1000 0000 | Зарезервирован, и может быть использован при поднятии max_ilev |

*Рис .1. Уровени целостности в ОС СН Astra Linux Smolensk Edition 1.6*

Таким образом, в ОС используется решетка уровней целостности (аналог решетки неиерархических категорий) в диапазоне значений от 0 до 255. Этот диапазон содержит набор несравнимых между собой уровней целостности (например, 1=0b00000001, 2=0b00000010, 4=0b00000100, 8=0b00001000, 16=0b00010000, 32=0b00100000, 64=0b01000000, 128=0b10000000), которые могут быть задействованы для системных сервисов (например, уровень целостности 8 зарезервирован для графического сервера Xorg). При установке ОС по умолчанию предлагается максимальный уровень целостности 63 (в двоичной системе 0b00111111), минимальный уровень всегда 0. Максимальными уровнями целостности в системе могут быть числа, у которых битовая маска включает битовые маски всех остальных используемых уровней целостности в системе (например, 63=0b00111111, 127=0b01111111, 191=0b10111111 и 255=0b11111111).

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. Просмотрите файл настроек загрузчика командой **cat /etc/default/grub** и найдите данный параметр. Также, убедитесь, что данный параметр был передан ядру при его настройке при загрузке командой **cat /proc/cmdline | grep "parsec.max_ilev"**. В выводе результата выполнения команды ненулевое значение параметра parsec.max_ilev означает, что режим включен.

Перейдем к практической отработке вопросов. Зайдем в систему с высоким уровнем целостности. Уровень целостности выбирается на этапе ввода логина и пароля (рис. 2).

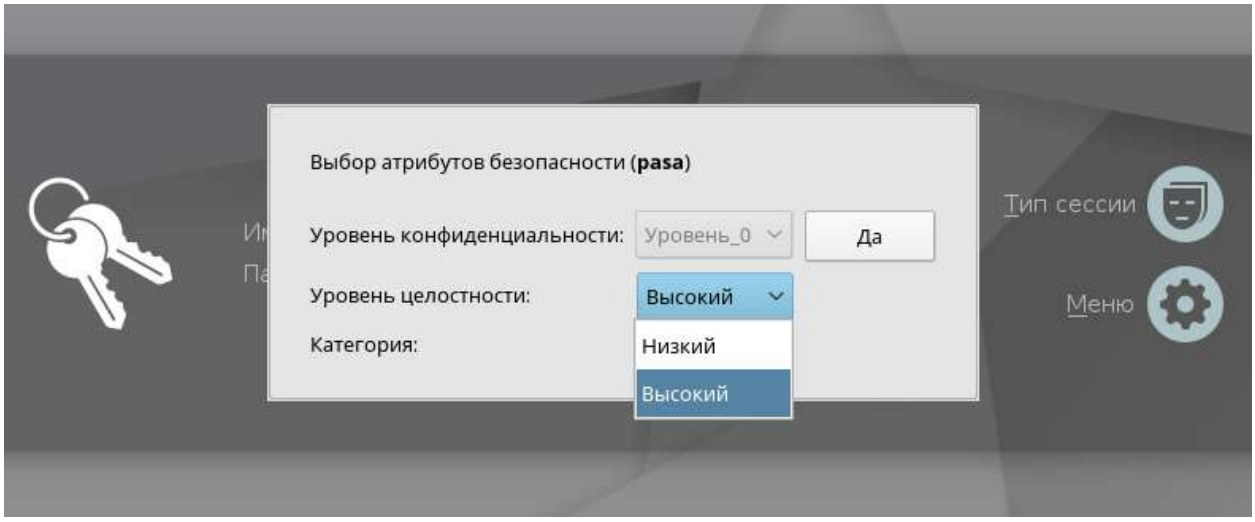


*Рис. 2. Этап выбора уровня целостности при входе в систему*

Уровню целостности 63 (высокому) соответствует красный цвет графического интерфейса fly (рис. 3)

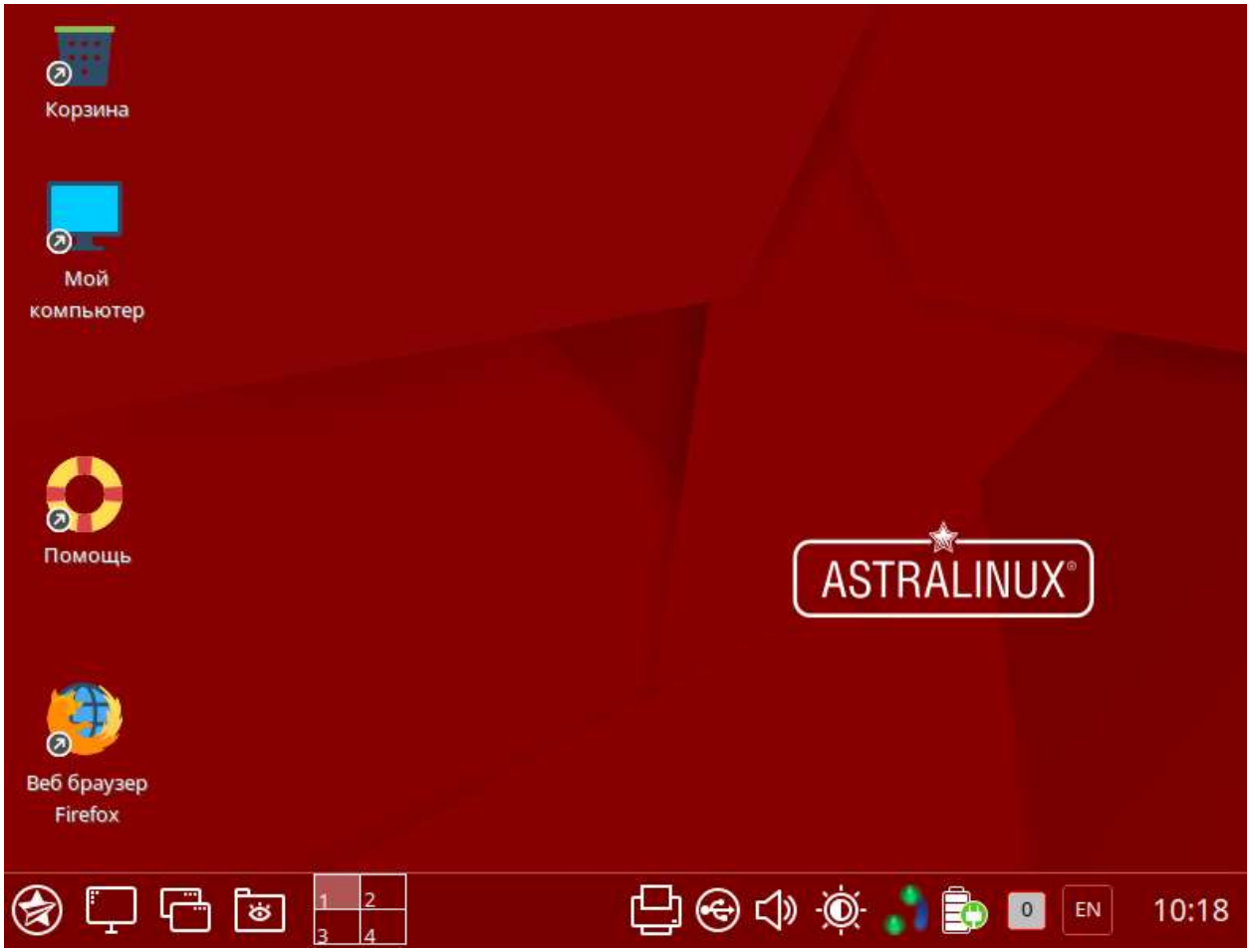


*Рис.3 . Интерфейс ОС при работе с высоким уровнем целостности*

**Средства управления мандатными ПРД**

Для управления мандатными ПРД используются следующие графические утилиты:

fly-fm («Менеджер файлов») – управление мандатными атрибутами файлов;

fly-admin-smc («Управление политикой безопасности») – управление протоколированием, привилегиями и мандатными атрибутами пользователей, работа с пользователями и группами.

Более подробное описание утилит см. в руководстве по КСЗ «Операционная система специального назначения «ASTRA LINUX SPECIAL EDITION»». Часть 1.

Для управления мандатными ПРД в режиме командной строки используются следующие утилиты:

pdpl-file – управление мандатными атрибутами файлов (см. 4.8.1 руководства);

pdp-id – отображение мандатных атрибутов сессии пользователя ОС (см. 4.8.2 руководства);

pdp-init-fs – скрипт инициализации мандатных атрибутов ФС (см. 4.8.3 руководства);

pdp-ls – вывод аналогично стандартной команде ls информации о файлах с отображением мандатных атрибутов (см. 4.8.4 руководства);

pdpl-ps – управление мандатными атрибутами процессов (см. 4.8.5 руководства);

pdpl-user – управление допустимыми мандатными уровнями и категориями пользователей ОС (см. 4.8.6 руководства);

sumac – запуск процесса с заданными мандатными уровнем и категорией в отдельной графической сессии (см. 4.8.7 руководства);

userlev – изменение БД мандатных уровней (см. 4.8.8 руководства);

usercat –изменение БД мандатных категорий (см. 4.8.9 руководства).

Для совместимости с предыдущими версиями ОС сохранены следующие утилиты командной строки для управления мандатными ПРД:

chmac – управление мандатными атрибутами файлов (см. 4.8.10.1 руководства);

lsm – вывод аналогично стандартной команде ls информации о файлах с отображением мандатных атрибутов (см. 4.8.10.3 руководства);

macid – отображение мандатных атрибутов сессии пользователя ОС (см. 4.8.10.2 руководства);

psmac – управление мандатными атрибутами процессов (см. 4.8.10.4 руководства);

usermac – управление допустимыми мандатными уровнями и категориями пользователей ОС (см. 4.8.10.5 руководства);

getfmac – получение мандатных меток файловых объектов (см. 4.8.10.6 руководства);

setfmac – изменение мандатных меток файловых объектов (см. 4.8.10.7 руководства).

Рассмотрим процесс настройки МКЦ при помощи графической утилиты fly-admin-smc. Утилита предназначена для управления протоколированием, привилегиями и мандатными атрибутами пользователей, работы с пользователями и группами.

Введите команду **sudo fly-admin-smc** или используйте «Панель управления» для запуска утилиты (рис. 4).


*Рис. 4. Интерфейс «Панель управления»*

В случае удачного запуска вы увидите интерфейс программы fly-admin-smc (рис. 5). Раскроем вкладку «Мандатный контроль целостности».

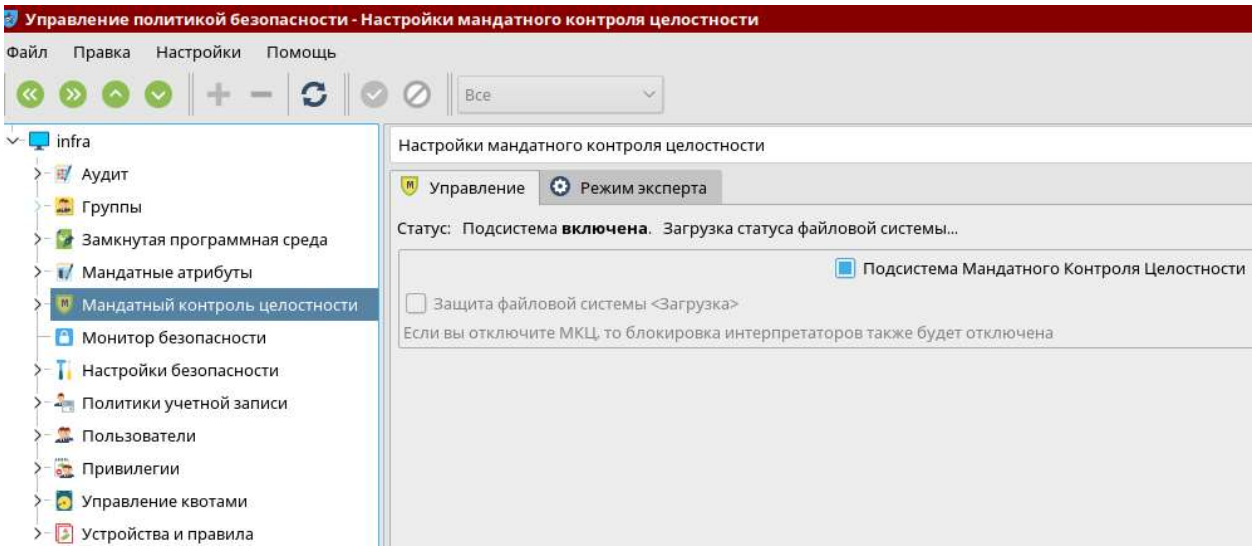


*Рис. 5. Интерфейс программы fly-admin-smc*

Перед началом любых настроек необходимо просмотреть настройки системы при помощи монитора безопасности. Перейдите на эту вкладку (рис. 6).

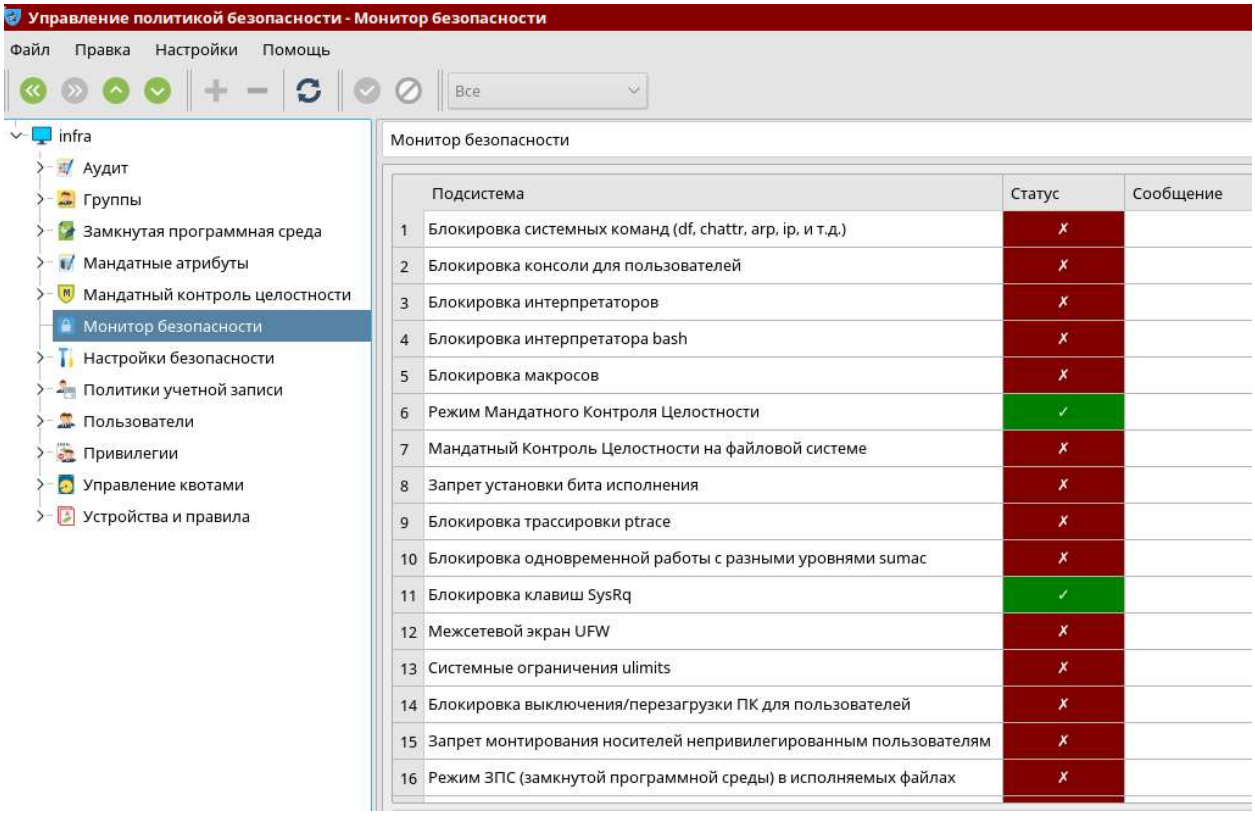


*Рис. 6. Интерфейс монитора безопасности при настройках ОС по умолчанию*

Красным цветом обозначаются невключённые и ненастроенные параметры безопасности. Зеленым цветом обозначаются включенные и настроенные параметры. Оливковым цветом обозначаются параметры, которые требуют дополнительной настройки, например, использование меток для ненастроенных файловых систем, ФС, смонтированных только на чтение, и т.п (см. скрипт /usr/sbin/pdp-init-fs).

Монитор безопасности очень часто используется контролирующими органами для оценки настроек параметров безопасности ОС. При этом монитор безопасности вашей ОС должен примерно соответствовать изображению, приведенному на рис. 7.

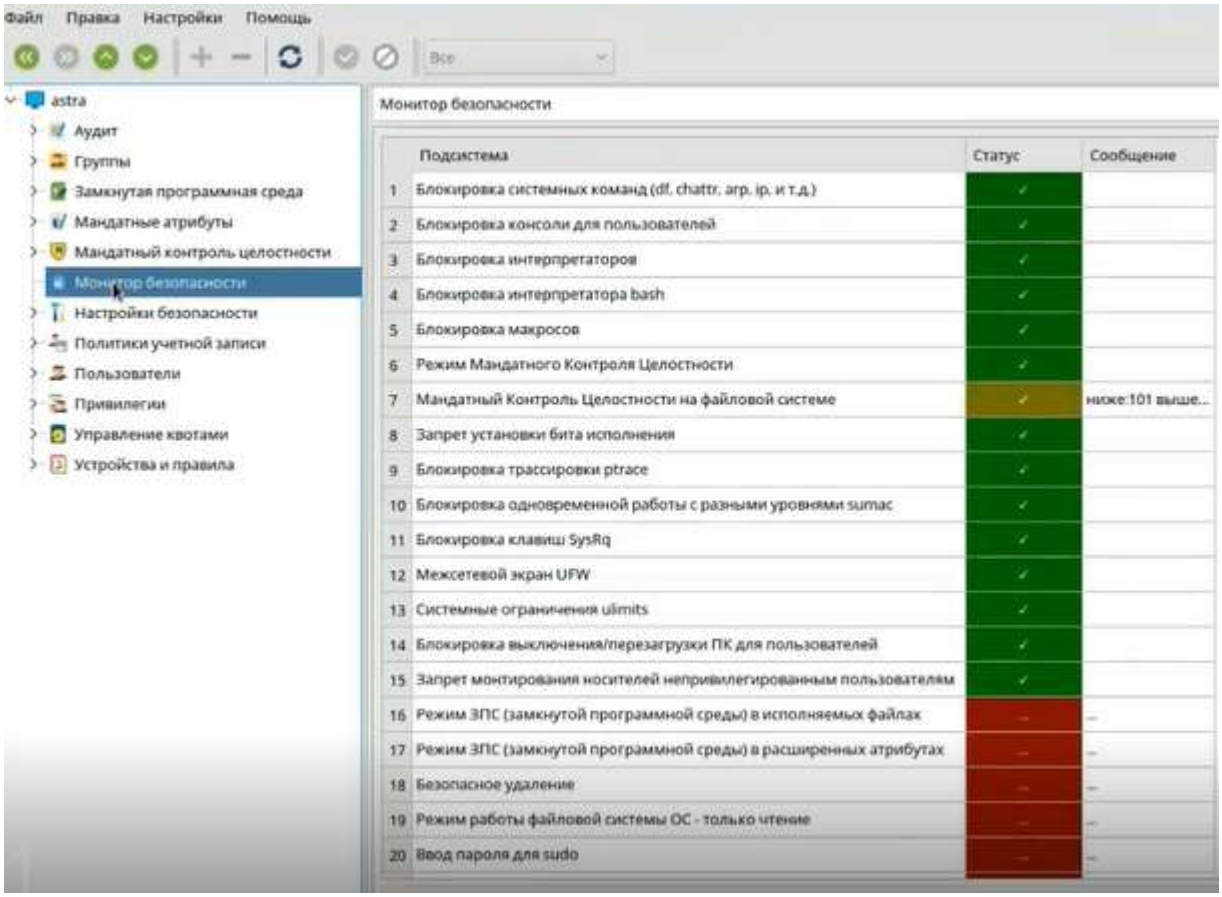


*Рис. 7. Интерфейс монитора безопасности после настройки ОС*

Для настройки необходимых параметров в окне интерфейса монитора безопасности выбираем нужный пункт и нажимаем на ставшую активной кнопку настройки нужных параметров (рис. 8)


*Рис.8 . Интерфейс монитора безопасности при настройке параметра МКЦ*

Перейдем к настройке МКЦ. Выбираем пункт меню «Мандатный контроль целостности на файловой системе», далее нажимаем кнопку «Настроить мандатный контроль….». Далее интерфейс настройки МКЦ зависит от

установленных обновлений безопасности. В данном курсе мы работаем с ОС с установленным обновлением номер 6 или выше. Как уже сказано выше, по умолчанию МКЦ включен, а защита ФС отключена (рис. 9).

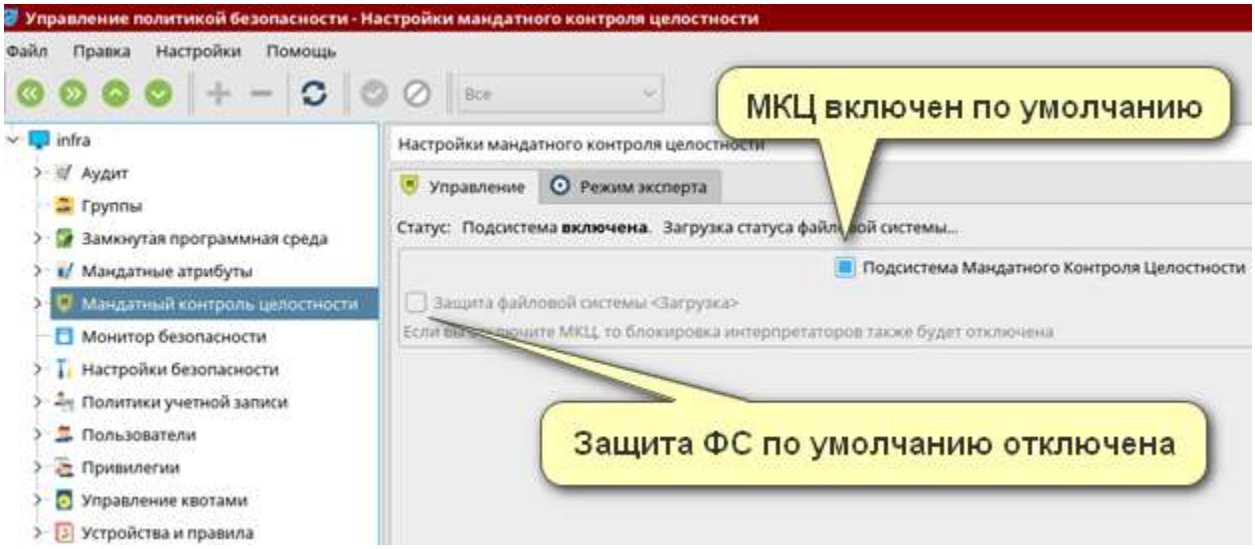


*Рис. 9. Настройки МКЦ по умолчанию*

Основные команды для настройки мандатного контроля целостности в ОС.

Проверить статус МКЦ в ОС можно командой **astra-mic-control status**.

Включение МКЦ на файловой системе производится командой **sudo astra-mic-control enable** или используя графическую утилиту fly-admin-smc. После включения МКЦ необходимо перезагрузить систему.

Теперь включим МКЦ на уровне файловой системы. Для этого используем команду **sudo set-fs-ilev**. Введите команду и после ее успешного выполнения, перезагрузите ОС, например, командой **init 6**. Проверим включение МКЦ на ФС при помощи монитора безопасности (рис. 10). Зеленый или оливковый цвет показывает, что все работает. Также, стал подсвечиваться синим цветом чекбокс «Защита файловой системы» на рисунке выше. МКЦ включается только для ФС таких как, ext2, ext3, ext4 и xfs.

| | Подсистема | Статус | Сообщение |
|---|---|---|---|
| 1 | Блокировка системных команд (df, chattr, arp, ip, и т.д.) | ✗ | |
| 2 | Блокировка консоли для пользователей | ✗ | |
| 3 | Блокировка интерпретаторов | ✗ | |
| 4 | Блокировка интерпретатора bash | ✗ | |
| 5 | Блокировка макросов | ✗ | |
| 6 | Режим Мандатного Контроля Целостности | ✓ | |
| 7 | Мандатный Контроль Целостности на файловой системе | ✓ | |
| 8 | Запрет установки бита исполнения | ✗ | |
| 9 | Блокировка трассировки ptrace | ✗ | |
| 10 | Блокировка одновременной работы с разными уровнями sumac | ✗ | |
| 11 | Блокировка клавиш SysRq | ✓ | |
| 12 | Межсетевой экран UFW | ✗ | |
| 13 | Системные ограничения ulimits | ✗ | |
| 14 | Блокировка выключения/перезагрузки ПК для пользователей | ✗ | |
| 15 | Запрет монтирования носителей непривилегированным пользователям | ✗ | |
| 16 | Режим ЗПС (замкнутой программной среды) в исполняемых файлах | ... | ... |
| 17 | Режим ЗПС (замкнутой программной среды) в расширенных атрибутах | ... | ... |
| 18 | Безопасное удаление | ... | ... |
| 19 | Режим работы файловой системы ОС - только чтение | ... | ... |
| 20 | Ввод пароля для sudo | ... | ... |

*Рис. 10. МКЦ ФС активирован*

Теперь рассмотрим какие настройки мы можем делать после включения МКЦ ФС.

Откроем вкладку «Мандатный контроль целостности» и перейдем в режим эксперта (рис. 11)

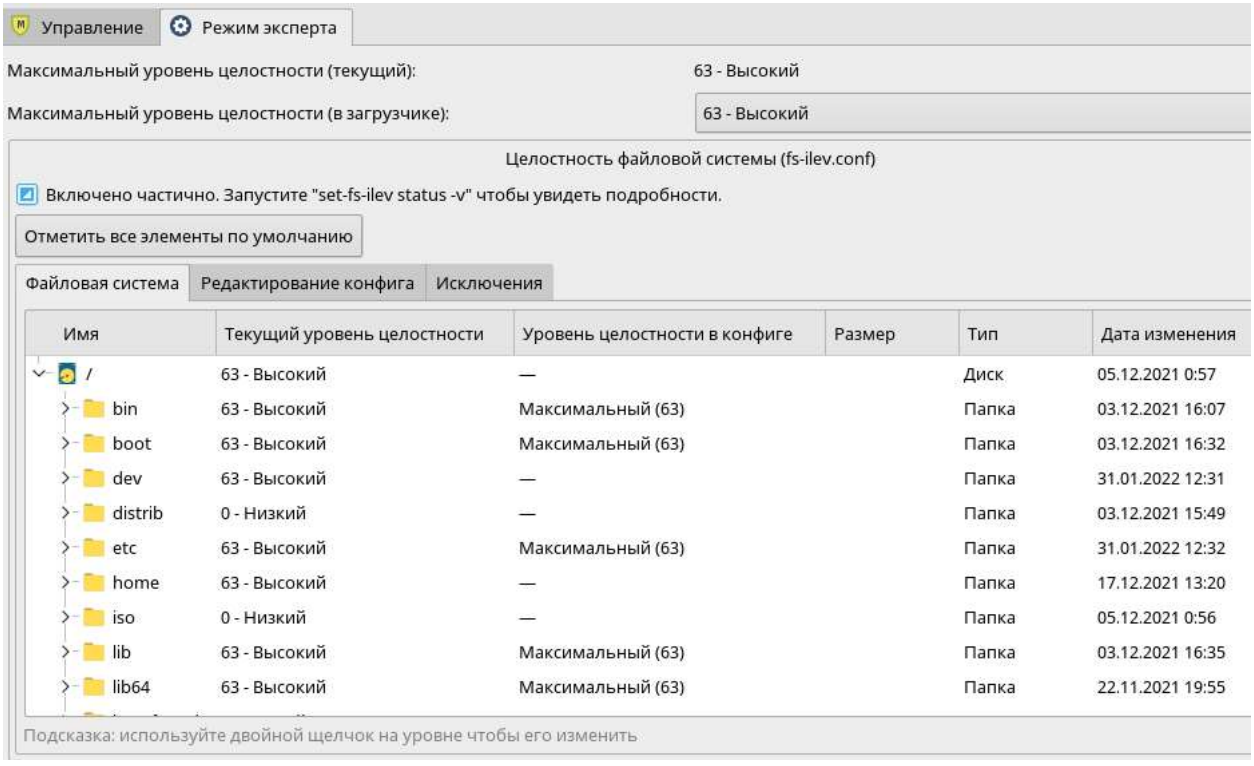

*Рис. 11. Режим эксперта*

Можно увидеть максимальный уровень целостности, установленный для ОС, а также просмотреть максимальный уровень целостности при загрузке. 127 уровень это виртуализация «Брест» (рис. 12).

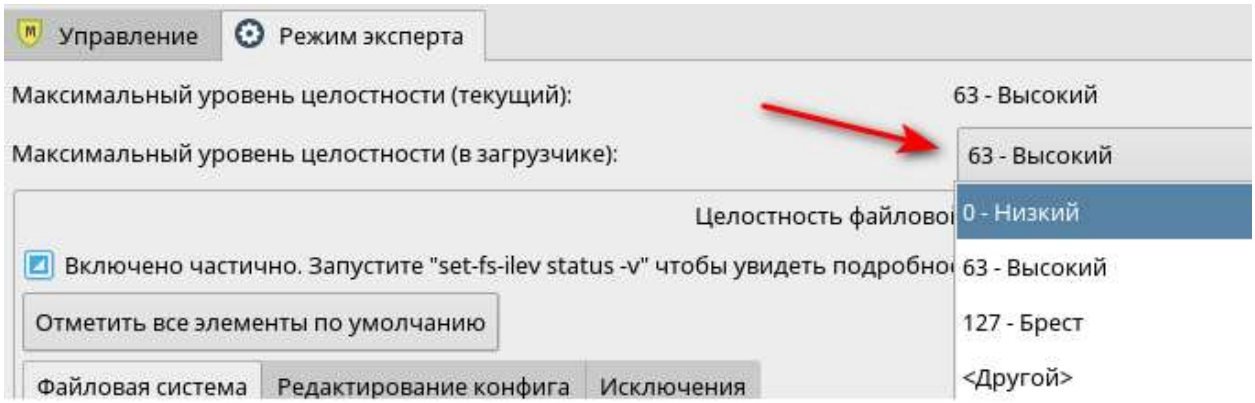


*Рис. 12. Режим эксперта. Выбор уровней целостности*

Также, в окне интерфейса режима эксперта отображена корневая файловая система. У каждого каталога есть свой текущий уровень целостности. У некоторых он равен 63, а у других – 0. Если, например, сейчас мы работает в высоком режиме КЦ, то нам доступны все каталоги. Например, если мы зайдем в ОС под учетной записью root, то нам будет запрещено вносить изменения в большинство каталогов, так как пользователь root в ОС Astra Linux Smolensk Edition 1.6 ограничен низким уровнем целостности (рис. 13). Такие ограничения учетной записи root связаны с необходимостью сертификации ОС по определенному классу защиты (по сути, в ОС Astra Linux Smolensk Edition 1.6 root не является администратором системы).

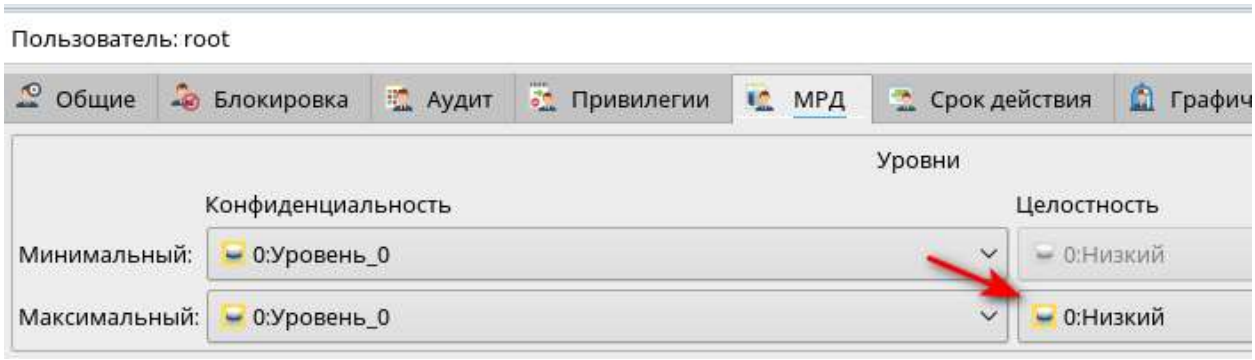


*Рис. 13. Уровень целостности пользователя root*

Редактирование уровней целостности для каталогов возможно во вкладке «Редактирование конфига» (рис. 14).

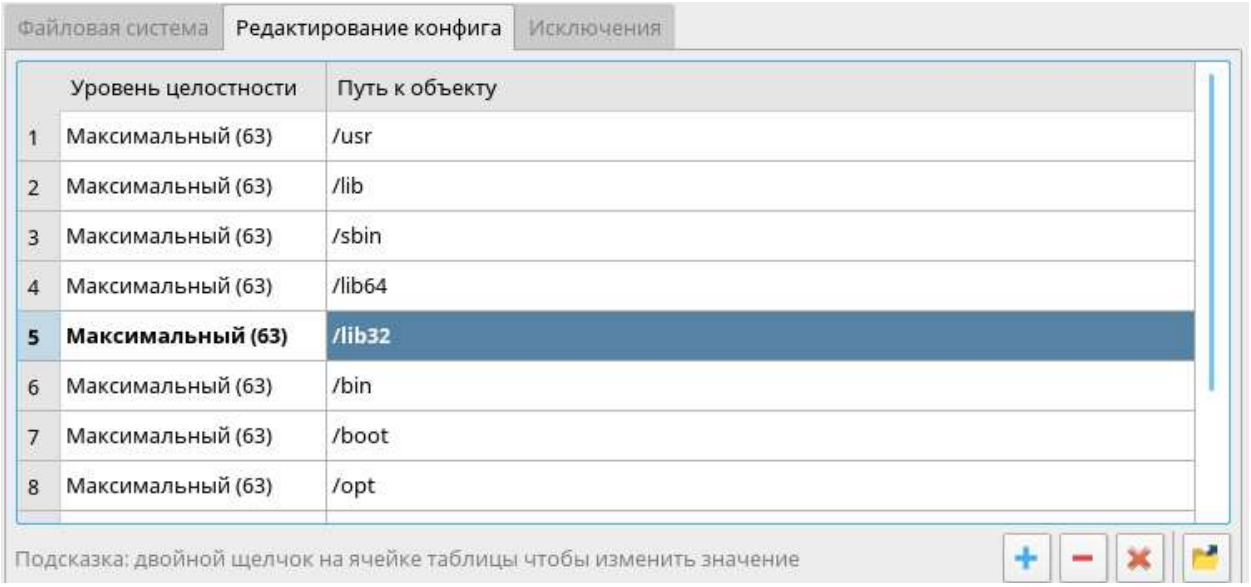


*Рис. 14. Уровни целостности для каталогов*

Для редактирования выбираем каталог и дальше можем устанавливать уровни целостности (рис.15). Чаще всего, уровни целостности для системных каталогов не меняются. Уровни настраиваются, как правило, для пользовательских каталогов, потому что для них при создании назначаются низкие уровни целостности.

Создайте какой-либо каталог, например, /proba. Проверьте его уровень целостности. Назначьте ему максимальный уровень целостности.

Внутри каталога с одним уровнем целостности нельзя создать каталог с другим уровнем целостности, за исключением случаем выставления специальной метки доступа. Тогда это становится возможным с ограничением, что внутри каталога можно создавать объекты с более низким уровнем целостности, но не выше уровня доступа каталога-родителя.

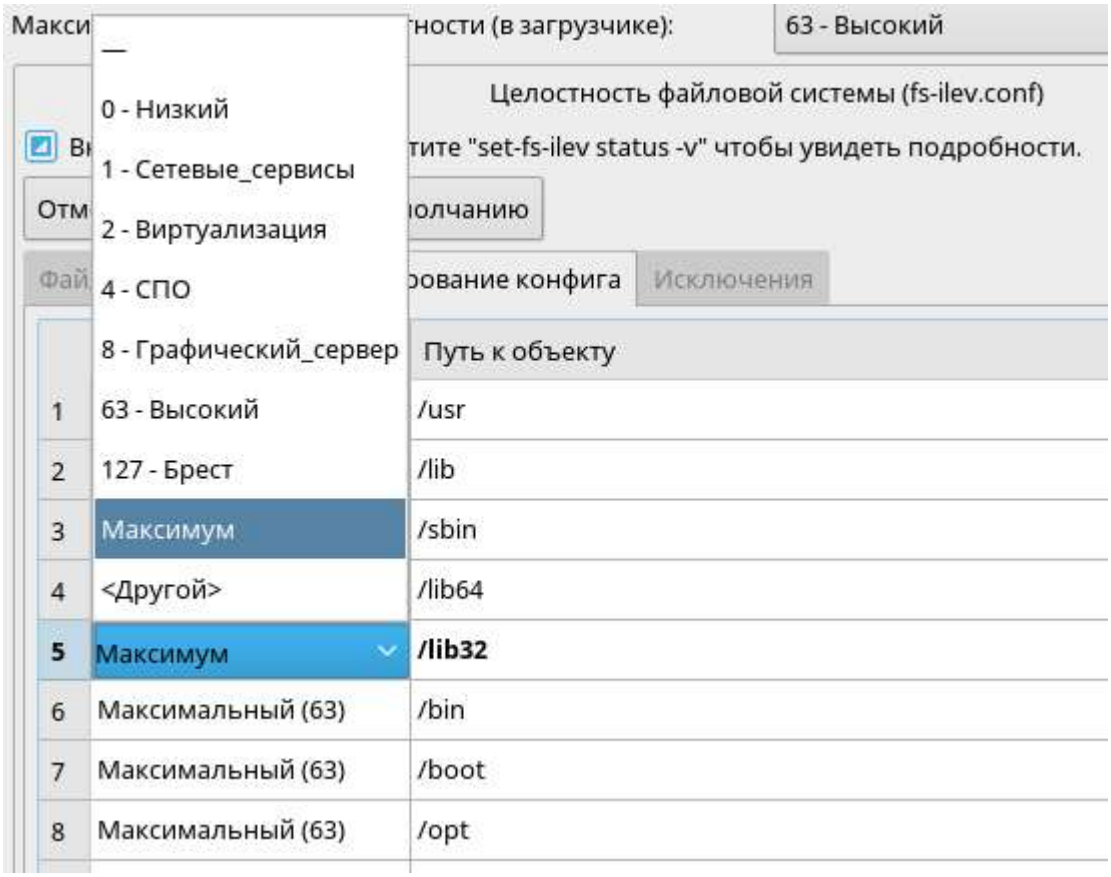


*Рис. 15. Выбор уровня целостности для каталога lib32*

В случае работы со старыми версиями ОС возможно редактирование МКЦ посредством скрипта инициализации мандатных атрибутов ФС. Скрипт находится по пути /usr/sbin/pdp-init-fs. Скрипт инициализации pdp-init-fs вызывается при инициализации и перезапуске системы для установки корректных мандатных атрибутов на системные файловые объекты (файлы и каталоги), начина с корня ФС.

Скрипт располагается в каталоге /usr/sbin и доступен для правки только администратору. Например, в нем можно исключить каталоги, назначенные для установки МКЦ, задать вручную максимальные уровни целостности для вложенных каталогов и многое другое.

Перед выключением режима МКЦ для ФС нужно снять атрибуты целостности с объектов файловой системы **sudo unset-fs-ilev** и перезагрузить систему. Далек выключение МКЦ на файловой системе производится командой **sudo astra-mic-control disable** или используя графическую утилиту fly-admin-smc (при этом автоматически удаляется соответствующий параметр parsec.max_ilev=63 из /etc/default/grub, но лучше в этом самому убедиться).

### Администрирование ОС при включенном режиме МКЦ

Непривилегированный пользователь может выполнять вход в систему только на низком уровне целостности (соответствует минимальному уровню

целостности). Привилегированный пользователь, при наличии соответствующего права, может входить в систему на высоком уровне целостности (соответствует максимальному уровню целостности ОС) и только для выполнения задач по конфигурированию ОС.

Любая настройка ОС при включенном режиме МКЦ выполняется при входе в систему на высоком уровне целостности. Обычный режим работы осуществляется на низком уровне целостности.

Администратор, созданный при установке ОС, может выполнять вход в систему с высоким уровнем целостности (по умолчанию 63) или с низким уровнем целостности. При графическом входе в систему для такого администратора по умолчанию выбран высокий уровень целостности. Графический рабочий стол на высоком уровне целостности имеет красный фон.

При консольном входе в систему администратор должен вручную выставлять уровень контроля целостности (для высокого уровня – 63, для низкого – 0 или пропустить данный шаг).

Включение МКЦ для ФС в системе производится командой sudo set-fs-ilev.

Перед включением режима МКЦ для ФС нужно снять атрибуты целостности с объектов файловой системы sudo unset-fs-ilev.

Выключение МКЦ на файловой системе производится командой **sudo astra-mic-control disable** или используя графическую утилиту fly-admin-smc

## Задание на выполнение лабораторной работы

Включите подсистему мандатного контроля целостности в ОС. Включите защиту ФС при загрузке. Проверьте статус систем подсистем при помощи консольных утилит. Создавайте каталог в ОС с именем как у вас. Назначьте ему максимальный уровень целостности. Самостоятельно создайте пользователя (используйте в качестве логина свою фамилию. Назначьте ему высокий контроль целостности. Настройте монитор безопасности на регистрацию событий, связанных с блокировкой трассировки ptrace, запрет монтирования носителей для непривилегированных пользователей, запрета установки бита исполнения).

## Литература

1. «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1»,

2. «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1».

3. «Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя».

Критерии выставления оценок обучающимся:

Знания, умения и навыки обучающихся определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Общими критериями, определяющими оценку знаний и умений обучающихся на текущем практическом занятии, являются:

«отлично» – наличие глубоких и исчерпывающих знаний в объеме материала практического занятия, правильные, уверенные действия по применению полученных знаний на практике, грамотное, логичное изложение материала при ответе.

«хорошо» – наличие твердых и достаточно полных знаний в объеме материала практического занятия, незначительные ошибки при освещении вопросов, правильные действия по применению знаний на практике, четкое изложение материала при ответе.

«удовлетворительно» – наличие твердых знаний в объеме материала практического занятия, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость в наводящих вопросах экзаменуемому, правильные действия по применению знаний на практике.

«неудовлетворительно» – наличие грубых ошибок в ответах, непонимание сущности излагаемых вопросов, неумении применять знания на практике, неуверенности и неточности в ответах на дополнительные и наводящие вопросы.

Порядок оценки выполнения задания

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

- название практического занятия;
- текст индивидуального задания;
- исходный текст программы;
- результаты тестирования решения.

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

подполковник С. Краснов
(воинское звание, подпись, инициал имени, фамилия автора)

«___»_____202_г.