Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

Специальность 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

**ОТЧЕТ**

**ПО УЧЕБНОЙ ПРАКТИКЕ**

Профессиональный модуль ПМ.01

*(наименование профессионального модуля)*

Выполнил:

обучающийся учебной группы № 1322

Маякин А.М.

*(И.О. Фамилия)*

Проверил:

руководитель практики от колледжа:

И.В. Сибирев

*(И.О. Фамилия)*

**Москва**

**20­­­­22**

**Перечень заданий/работ, выполненных в ходе учебной практики**

Специальность 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

*(наименование специальности)*

Профессиональный модуль ПМ.01

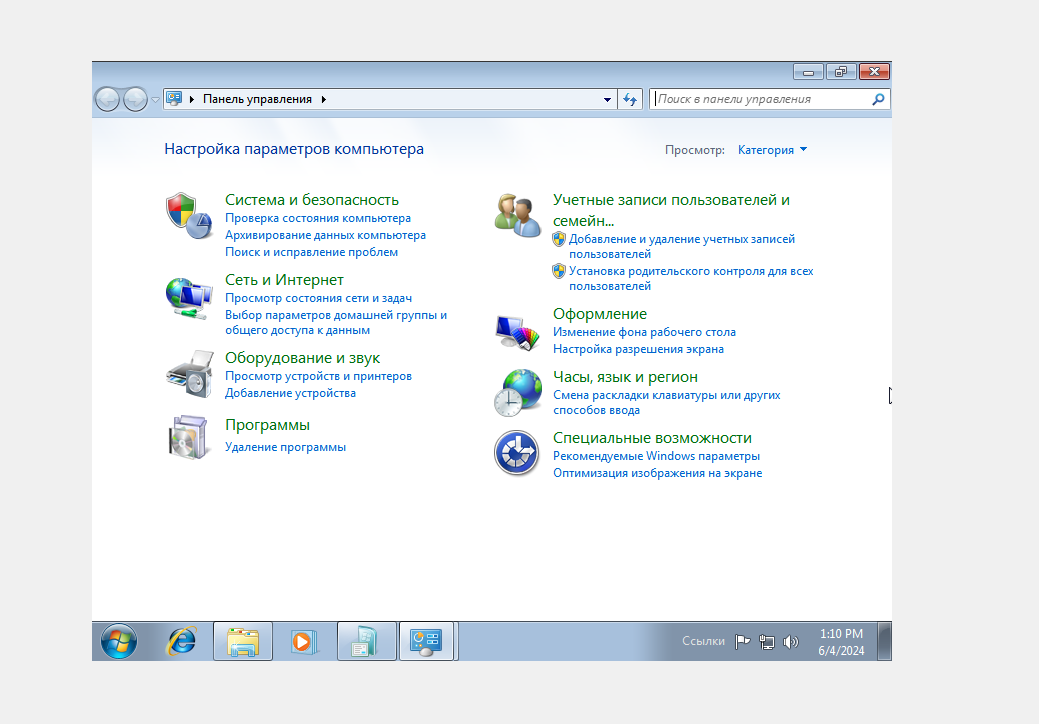
*(наименование профессионального модуля)*

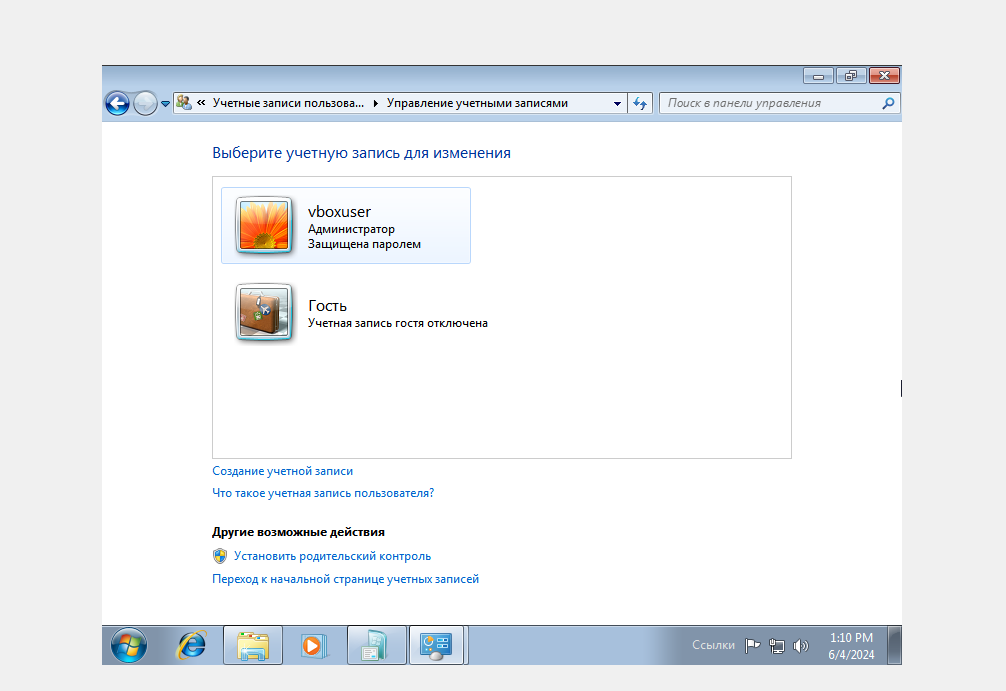
|  |  |  |
| --- | --- | --- |
| Номер работы | Темы учебной практики | Выполненные задания |
| 1 | Управление учётными записями пользователя | Сформировали навыки по созданию и управлению учётными записями пользователей. |
| 2 | Настройка Windows Server 2016 | Сделали конспект по теме |
| 3 | Создание и настройка параметров мандатного управления доступом | Оформили отчёт при работе на платформе ОС Astra Linux |
| 4 | Управление мандатным доступом | Сделали конспект |

**Практическая часть**

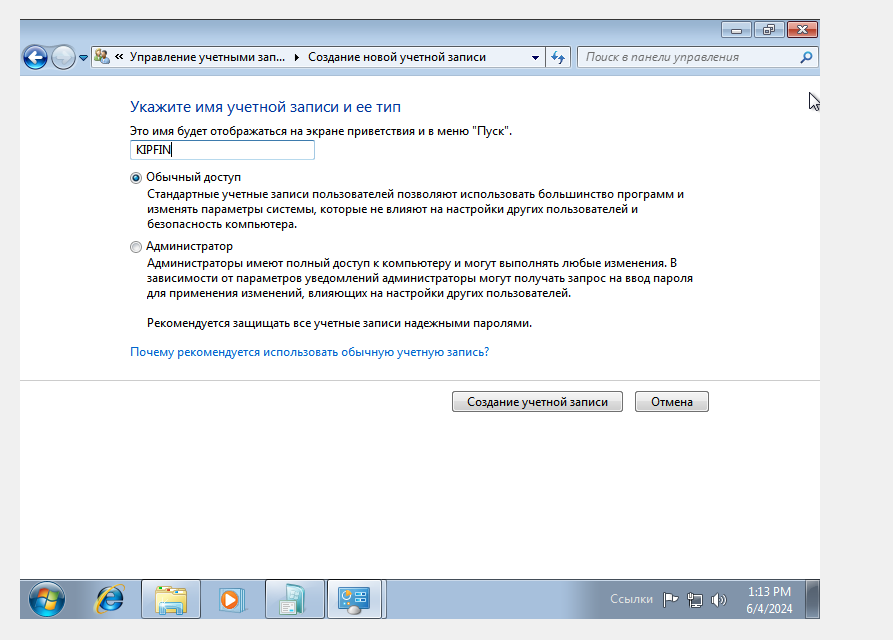
Работа 1. Управление учётными записями пользователя

1. Установил 7 Windows
2. Для перехода в режим настройки и редактирования учетных записей необходимо в панели управления выбрать категорию Учетные записи пользователей, и в этой категории щелкнуть на ссылке Добавление и изменение учетных записей пользователей.

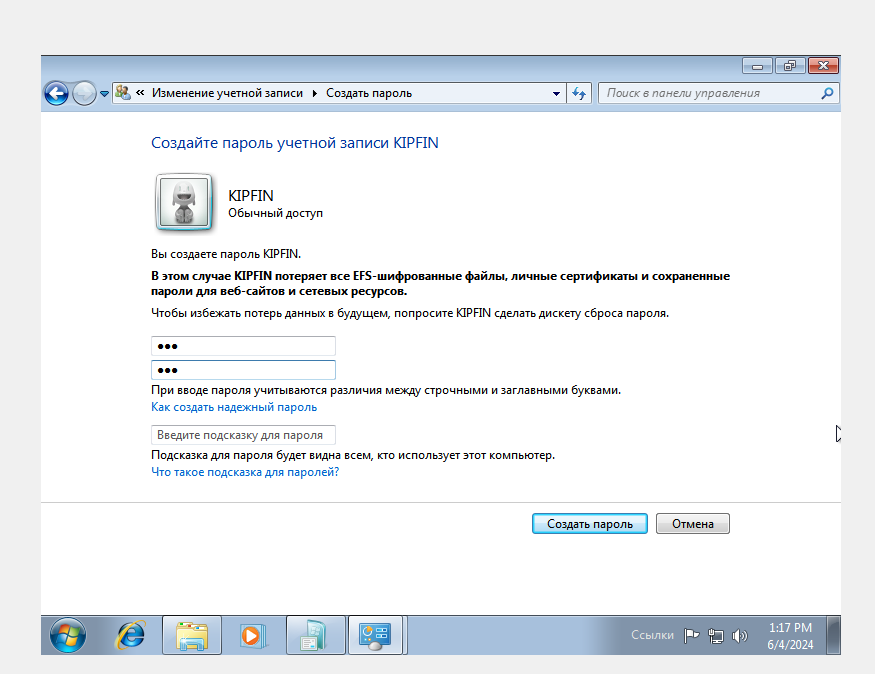




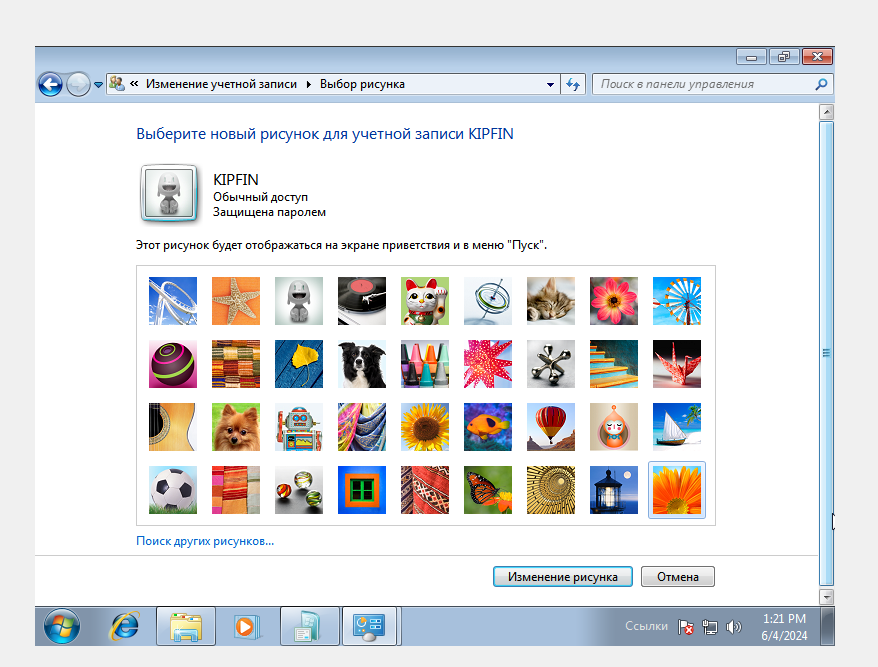
1. Далее создаем новую учебную запись и ставим имя KIPFIN



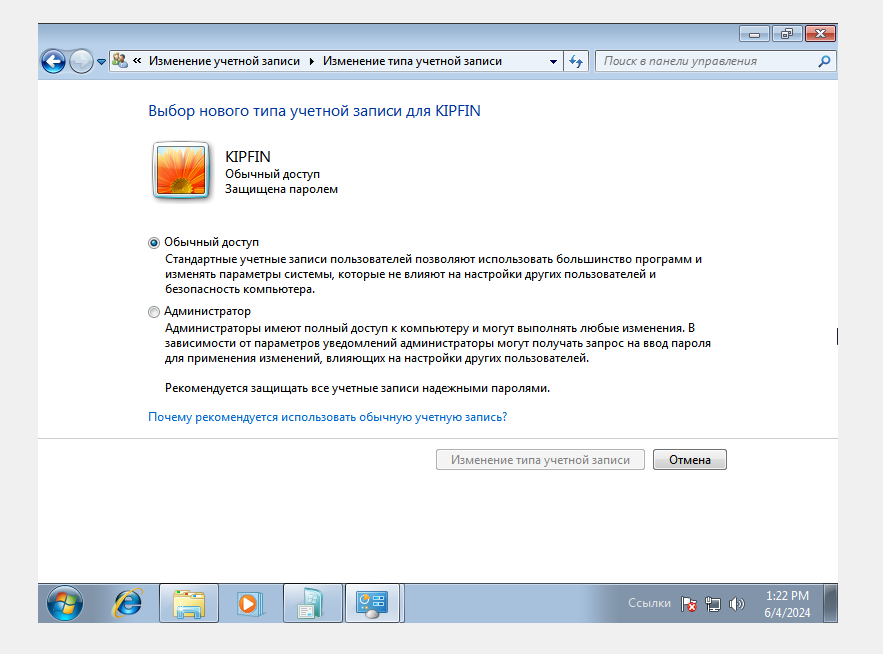
Изменяем нашу учетную запись, меняем пароль, ставим пароль 123



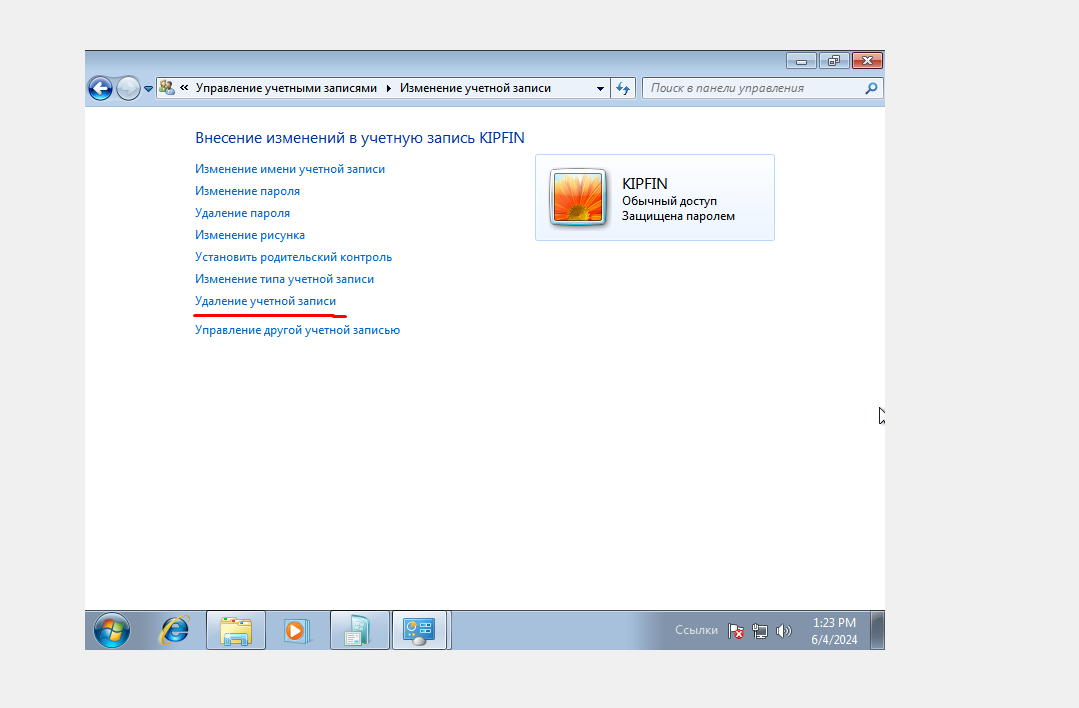
Изменяем аватарку нашего пользователя



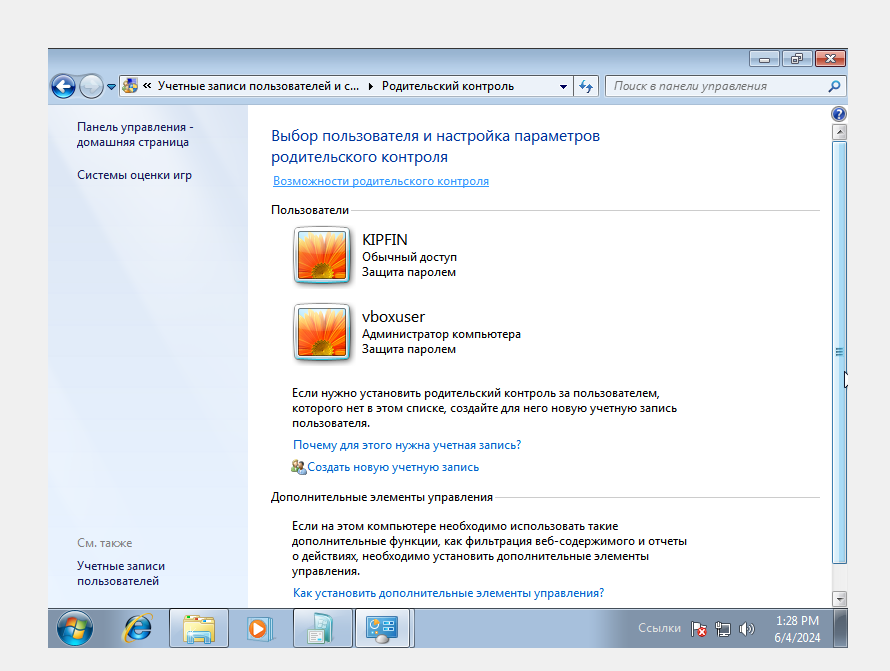
Далее можем изменить тип учетной записи, но я не буду этого делать



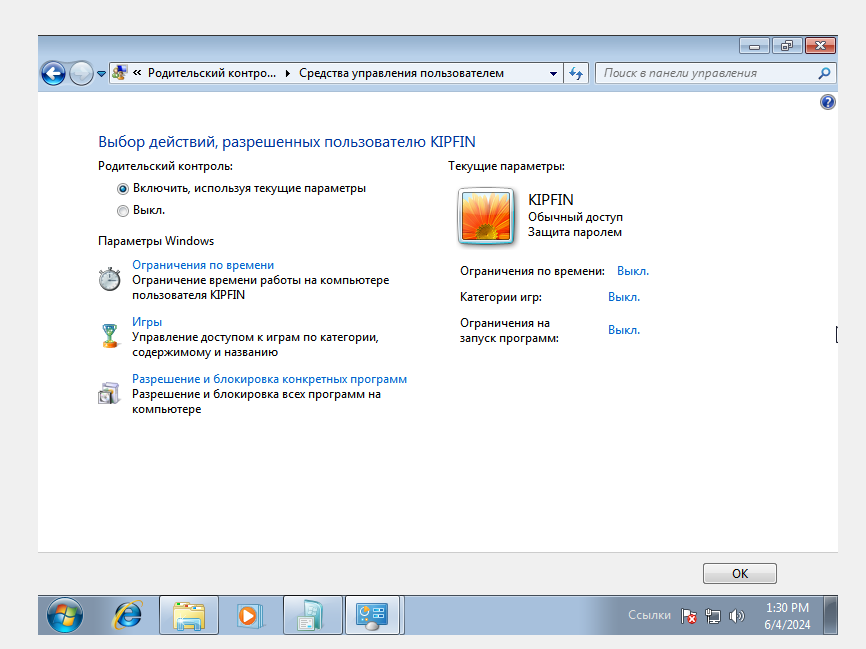
Далее можем удалить учетную запись, но мы этого не будем делать



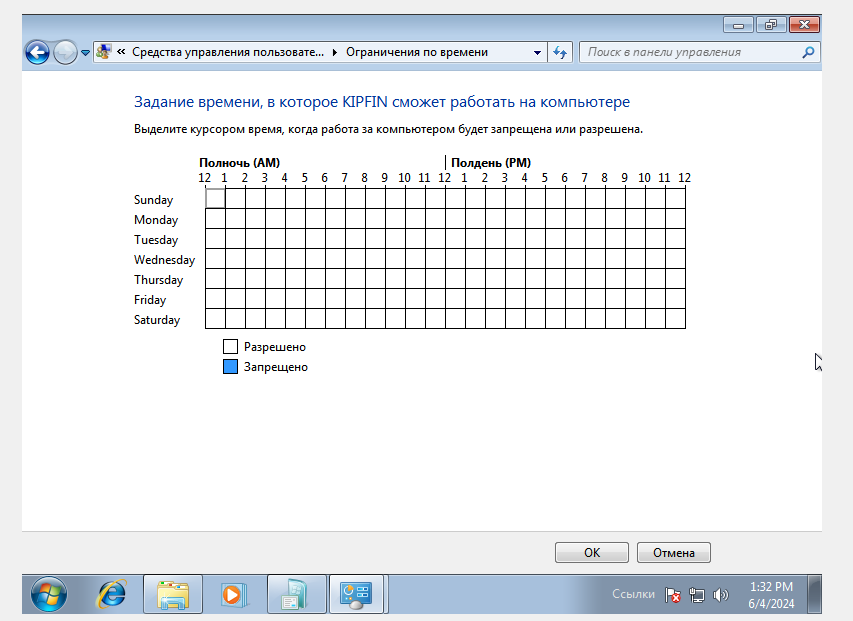
Далее переходим в родительский контроль и выбираем учетную запись KIPFIN



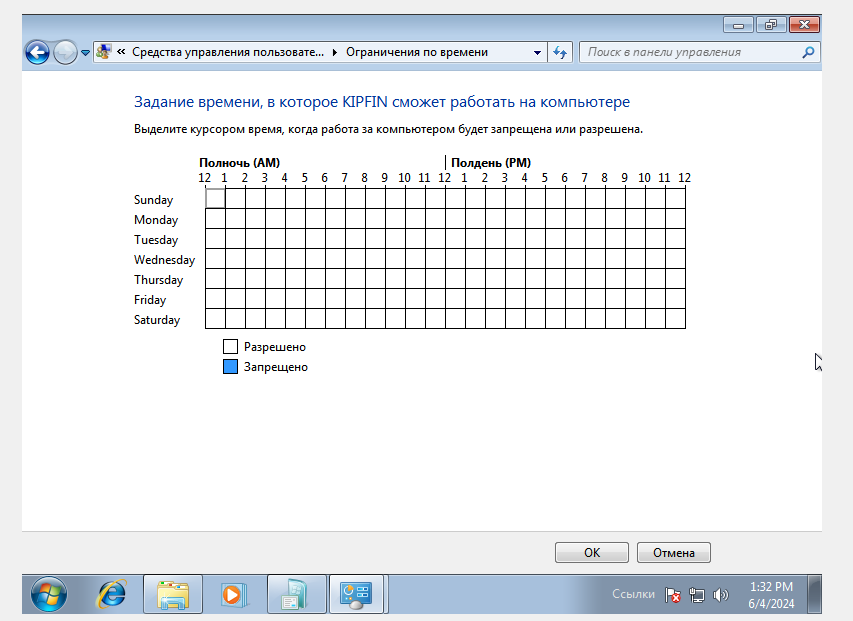
И Включаем родительский контроль



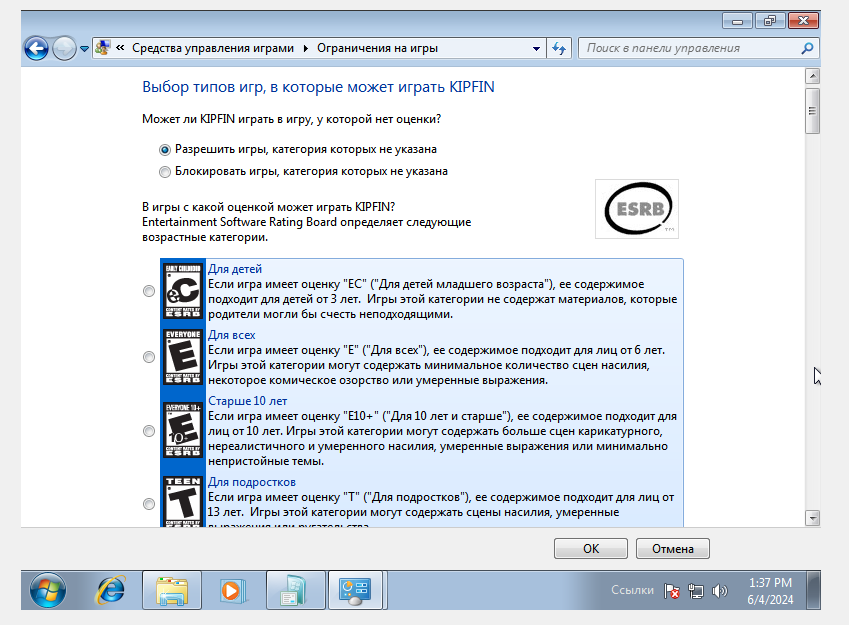
Далее мы можем ограничить по времени использования компьютера, но я этого не буду делать



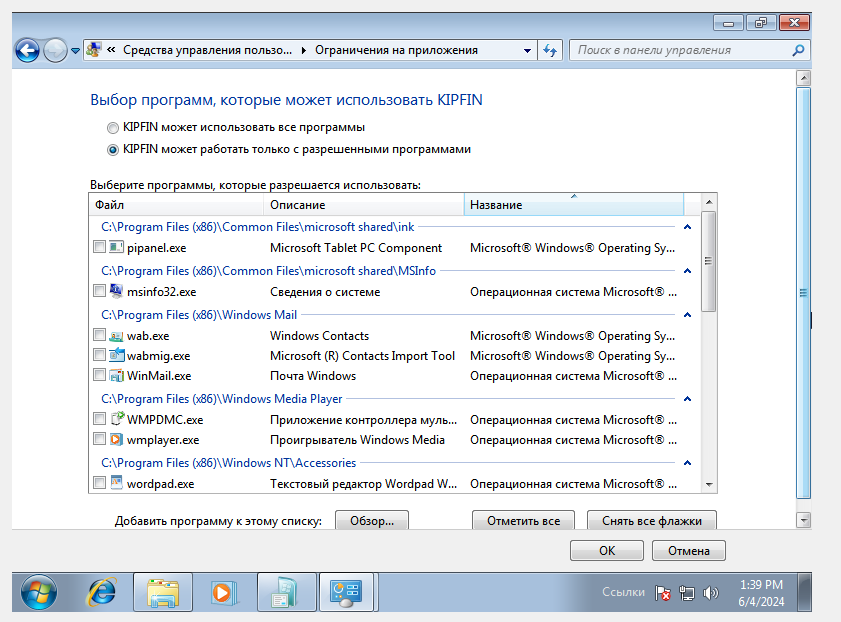
Далее можем ограничить пользованием игр



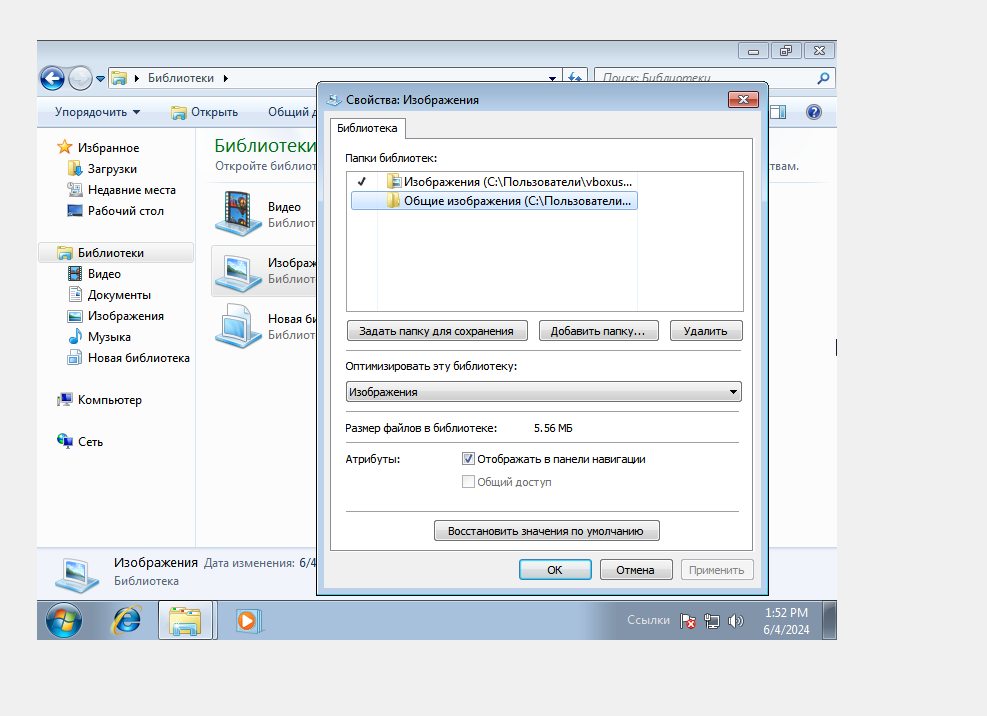
Можем задать категорию игр



Так же мы можем выбрать программы, которые можно использовать, а какие нет



Я не смог настроить безопасность файла, ибо когда пытаешься открыть свойства файла, там нет иконки безопасность.



Задание 2.

**Лабораторный стенд представлен сервером на базе Windows Server 2016 и клиентской машиной на базе Windows 10. Забегая вперед, скажу, что на сервере подняты роли активной директории и файлового сервера, клиентский компьютер добавлен в домен. оздадим общий ресурс на файловом сервере. Для этого в диспетчере серверов перейдем в раздел общие ресурсы. Щелкнем правой кнопкой мыши и создаем ресурс, оставляя при этом параметры по умолчанию.**

**Далее создадим необходимые элементы в Active Directory Windows Server 2016. Создадим новое подразделение в домене. Откроем оснастку пользователи и компьютеры. Щелкнем на домен “vlab.edu” и создаем подразделение. Назовем его “vlab”.**

**В этом подразделении аналогично создадим нового пользователя “user1”. Под ним мы будем входить в домен на клиентской машине. И создадим группу “NetDrive”, в разделе групп, в последствии добавив в нее нашего пользователя. Эта группа понадобиться нам как фильтр безопасности для применения групповой политики.**

**Создадим объект групповой политики. Откроем оснастку «Управление групповой политикой» и в разделе объектов создадим новую. Назовем ее «AddNetDrive».**

**Теперь давайте изменим ее содержимое. В разделе конфигурации пользователя, необходимо открыть раздел настроек, далее конфигурации windows и выбрать сопоставление дисков. Создадим элемент «сопоставленный диск». В параметрах укажем путь к общему ресурсу, в нашем случае это \\ad1\share, укажем букву диска, и обязательно установим галочку «выполнять в контексте пользователя». Привяжем объект к нашему подразделению … и укажем в фильтре безопасности созданную ранее группу.**

**Вводим учетные данные и входим в систему под доменной учетной записью “user1”. Проверяем подключился ли у нас сетевой диск. Диск подключен. Но обращаю ваше внимание что на этом диске доступно столько же пространства сколько и на родительском диске общего файлового ресурса. Что бы не допустить переполнения, нам необходимо установить квоту.**

**Давайте перейдем к ее созданию. Для того что бы создать квоту, необходимо открыть диспетчер ресурсов файлового сервера. В разделе квот создаем новую квоту и назначаем ей параметры по умолчанию, выбирая их из шаблона.**

**Этого вполне достаточно что бы изучить принцип действия квотирования и понять, как он функционирует. Если вас интересую вопросы по «тонкой» настройке квот, оставляйте их в комментариях под видео, постараюсь всем ответить.**

**Вернемся на клиентский ПК и удостоверимся что квота применена и функционирует. Доступное для использования общего ресурса пространство ограничено размером в 100МБ. И теперь чисто технический используя этот сетевой ресурс допустить переполнения родительского диска невозможно**

**Итог: на мой взгляд данная технология позволяет более эффективно использовать ресурсы сервера и осуществлять мониторинг и контроль рационального использования дискового пространства. К тому же она позволяет избежать ряда проблем связанных с переполнением дисков.**

Задание 3.

**Цель лабораторной работы**

Изучить и освоить администрирование основных параметров мандатного управления доступом в ОССН Astra Linux Special Edition с применением графических утилит и консольных команд.

**Используемое программное обеспечение**

Для выполнения лабораторной работы используется установленный дистрибутив ОС Astra Linux  Smolensk.

**Задание на лабораторную работу**

В ходе лабораторной работы необходимо произвести установку и настройку пакетов OpenLDAP, Kerberos, NSS, PAM, NFS, SMB, NMBD.

***Практическая часть***

Отключили блокировку экрана.

Создали учётную запись user с паролем Student123. Добавили учётную запись user во вторичную группу astra-admin (рис 1)

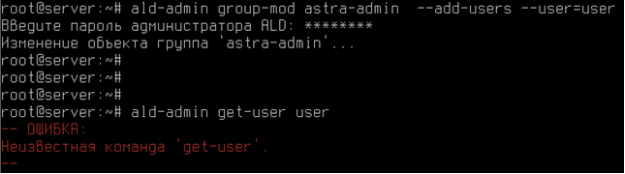


Рисунок 1

Начали работу со входа в ОССН в графическом режиме с учётной записью пользователей “Управление политикой безопасности” через команду sudo fly-admin-smc (рис 2)

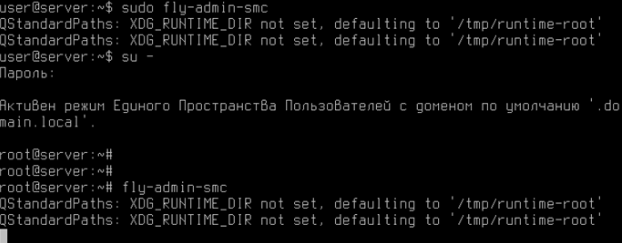


Рисунок 2

Модифицировали параметры мандатного управления доступом (рис 3)

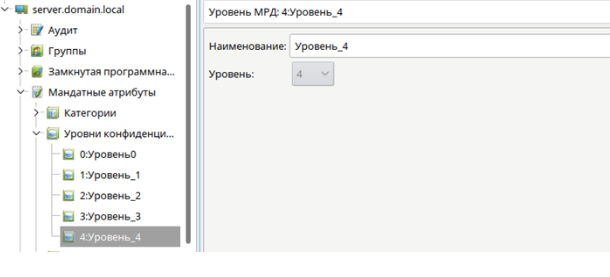


Рисунок 3

Создали учётную запись пользователя user1, установив максимальный уровень доступа (рис 4)

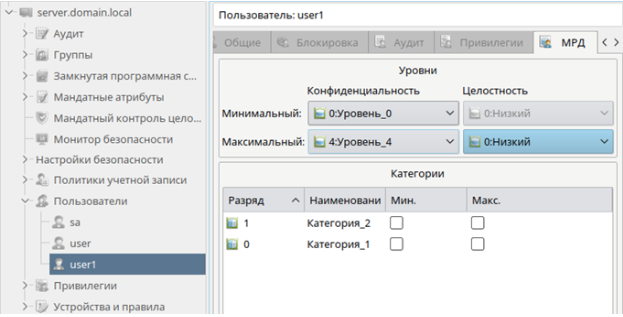


Рисунок 4

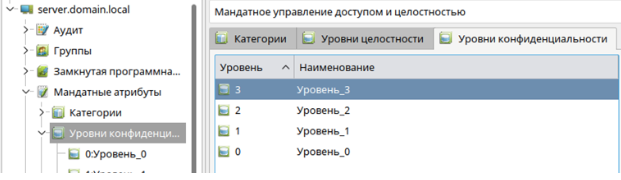


Рисунок 5

Открыть учётную запись пользователя user1 и в закладке «Дополнительные» в элементе «Максимальный уровень» проверить наличие записи «(4)», при этом, в списке выбора уровня «Уровень\_4» будет отсутствовать. Создать учетные записи user20, user30, user40. Задать в произвольном порядке значения для параметров «Конфиденциальность», «Целостность», «Категории».

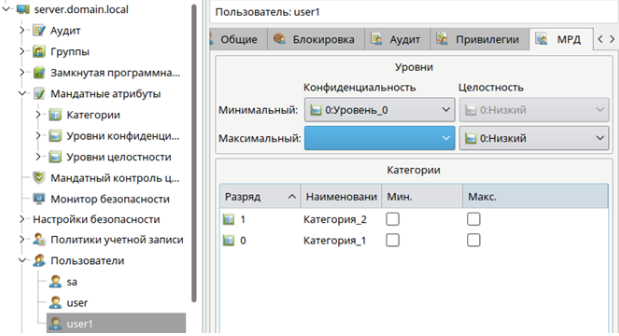


Рисунок 6

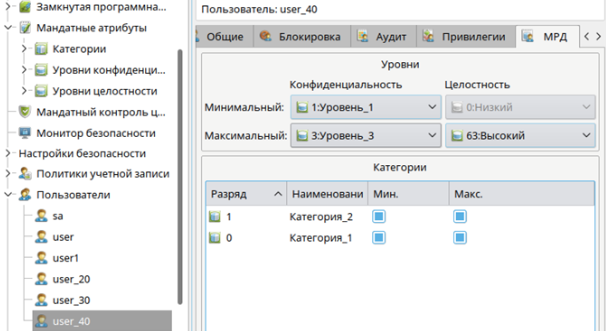


Рисунок 7

Ознакомится с содержимым каталога etc/parsec/macdb. Вывести в терминал Fly параметры мандатного управления доступом для учётной записи пользователей user1, user20, user30, user40. Мандатные атрибуты, назначенные конкретным учётным записям пользователей, перечисляются в каталоге /etc/parsec/macdb. Для выполнения задания 7 осуществить следующие действия:

* 1. запустить терминал Fly и перейти в каталог /etc/parsec/macdb (команда cd /etc/parsec/macdb )
  2. вывести на экран содержимое каталога /macdb ( ls )
  3. просмотреть содержимое файлов в каталоге /macdb ( sudo cat “имя файла” )
  4. прочитать параметры учётной записи user1 командой sudo grep “user1” \*
  5. определить максимальный уровень доступа учётной записи user1 командой sudo grep «user1» \* | cut -d : -f 5
  6. определить минимальный уровень доступа учётной записи user1 командой sudo grep «user1» \* | cut -d : -f 3 и проверить его соответствие данным, отображаемым в графической утилите «Управление политикой безопасности».

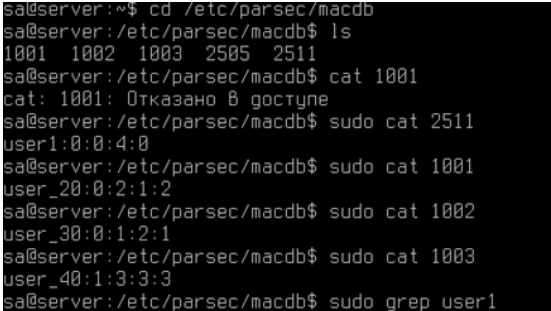


Рисунок 8

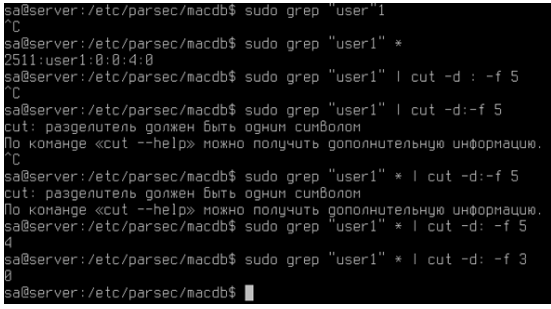


Рисунок 9

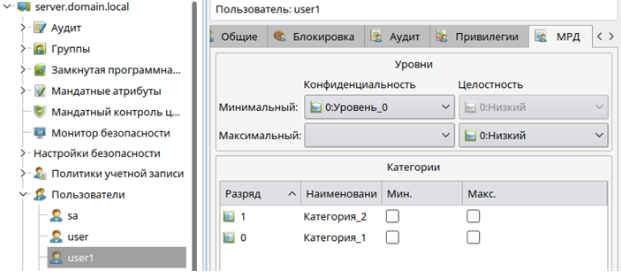


Рисунок 10

Создать неиерархические категории с использованием графической утилиты «Управление политикой безопасности». Для этого выполнить следующие действия:

* 1. в разделе «Категории» удалить все Категории.
  2. в разделе «Категории» создать новую неиерархическую категорию с именем «Otdel1», «Разряд» — 0;
  3. в разделе «Категории» создать новые неиерархические категории: «Otdel2» («Разряд» — 1), «Upravlenie» («Разряд» — 2).

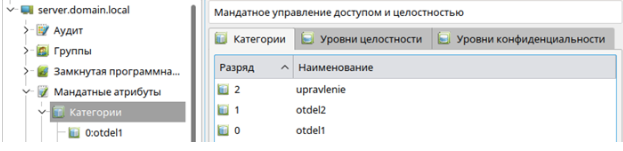


Рисунок 11

Изменить набор неиерархических категорий с использованием графической утилиты «Управление политикой безопасности» (sudo fly-admin-smc), для этого выполнить следующие действия в разделе «Категории»:

* 1. выбрать неиерархическую категорию «Otdel1» и ввести наименование «Отдел\_1»;
  2. аналогично переименовать неиерархические категории «Otdel2» и «Upravlenie» в «Отдел\_2» и «Управление» соответственно;
  3. проанализировать возможность одновременного изменения элемента «Разряд».

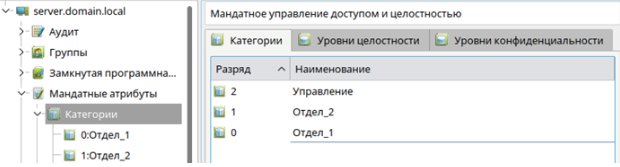


Рисунок 12

Изменить мандатный уровень доступа с использованием графической утилиты «Управление политикой безопасности», для этого выполнить следующие действия:

* 1. создать новую группу с именем «office1» и задать первичную группу учётной записи пользователя user1 — «office1»;
  2. создать новую учетную запись пользователя user2 и установить её первичную группу — «officel»;
  3. в закладке «МРД» осуществить попытку выбора минимального набора неиерархических категорий — «Отдел\_2» и проанализировать результат;
  4. в закладке «МРД» выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_2», после чего задать минимальный набор неиерархических категорий — «Отдел\_2»;
  5. открыть параметры учётной записи пользователя user1 и выбрать максимальный уровень доступа — «Уровень\_3», максимальный набор неиерархических категорий — «Отдел\_1», минимальный набор неиерархических категорий — «Отдел\_1»;.
  6. создать учётную запись пользователя rukoffice1 и задать первичную группу: «office1» ;
  7. в закладке «МРД» выбрать максимальный уровень: «Уровень\_3», максимальный набор категорий: «Отдел\_1», «Отдел\_2», «Управление».

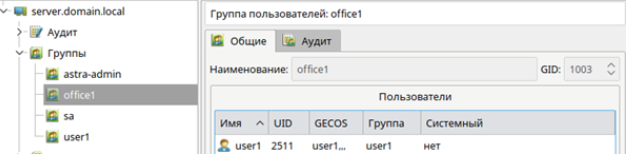


Рисунок 13

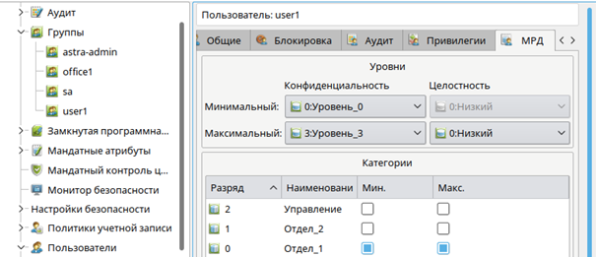


Рисунок 14

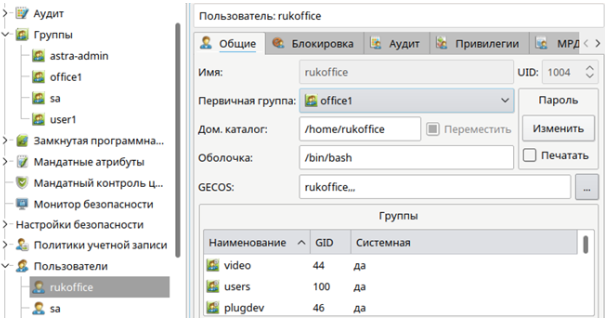


Рисунок 15

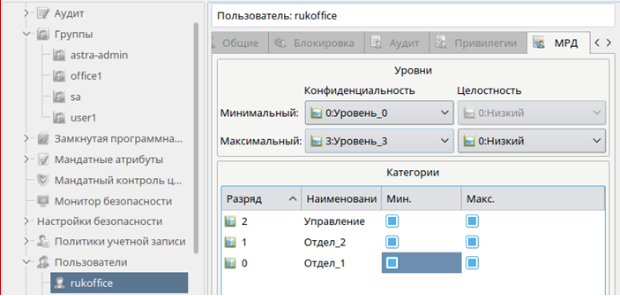


Рисунок 16

Создать общий каталог для работы от имени учётных записей пользователей userl, user2, rukoffice1 в каталоге /home/work. Для работы от имени учётных записей пользователей с наборами неиерархическими категорий «Отдел\_1», «Отдел\_2» и «Управление» выделить отдельные каталоги «otdel1», «otdel2» и «upr» соответственно.

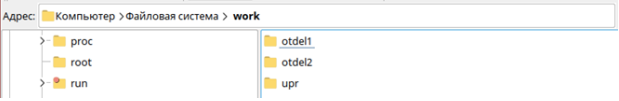


Рисунок 17

При этом обеспечить хранение файлов с различными уровнями конфиденциальности в каталогах с использованием специального атрибута CCNR, для чего осуществить следующие действия:

* 1. запустить терминал Fly в «привилегированном» режиме командой sudo fly-term;
  2. Прочесть информацию по командам mkdir, chown и chmode в приложении для практической работы.
  3. создать каталог work и задать параметры мандатного и дискреционного управления доступом командами:

*mkdir /home/work*

*chown user /home/work -v (назначение user владельцем каталога)*

*ls –lh (посмотрите изменения параметра “владелец” для каталога work)*

*chown :office1 /home/work –v (назначение группы)*

*ls –lh (посмотрите изменения параметра “группа” для каталога work)*

*chmod 750 /home/work*

*pdp-flbl 3:0:Отдел\_1,Отдел\_2,Управление:ccnr /home/work –v*

* 1. создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий «Отдел\_1» и задать параметры мандатного и дискреционного управления доступом командами:

*cd /home/work*

*mkdir otdel1*

*chown user1:office1 otdel1*

*chmod 770 otdel1*

*pdp-flbl 3:0:Отдел\_1:ccnr otdel1*

* 1. создать каталог для работы от имени учётных записей пользователей с набором неиерархических категорий «Отдел\_2» и задать параметры мандатного и дискреционного управления доступом командами:

*mkdir otdel2*

*chown user2:office1 otdel2*

*chmod 770 otdel2*

*pdp-flbl 3:0:Отдел\_2:ccnr otdel2*

* 1. создать каталог upr для работы от имени учётных записей пользователей с набором неиерархических категорий «Управление» командами:

*mkdir upr*

*chown rukoffice1:office1 upr*

*chmod 770 upr*

*pdp-flbl 3:0:Управление:ccnr upr*

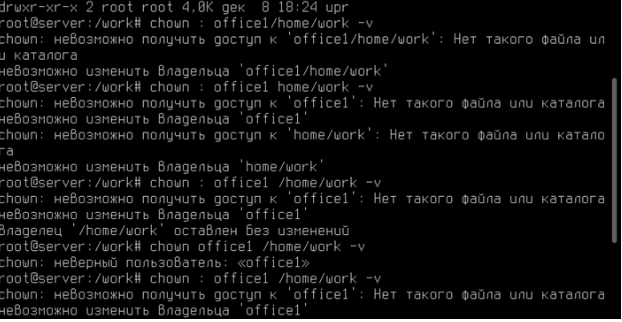


Рисунок 18

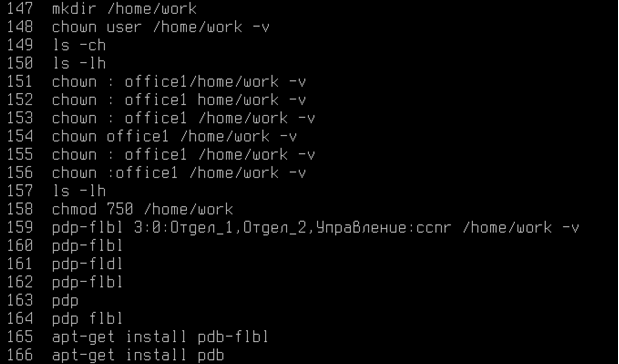


Рисунок 19

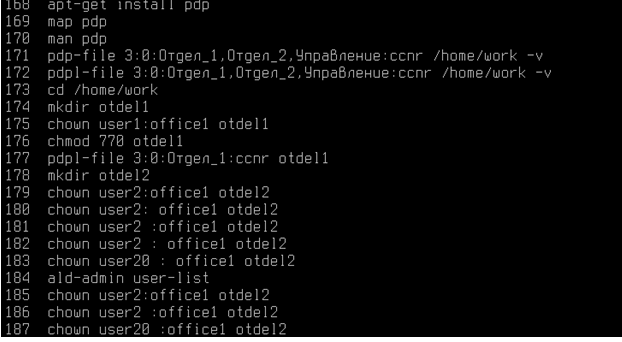


Рисунок 20

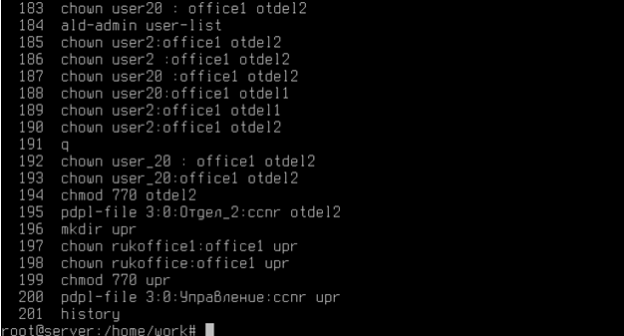


Рисунок 21

Задание 4.

Мандатный контроль целостности (Mandatory Access Control, MAC) в операционной системе Astra Linux представляет собой механизм, который обеспечивает контроль доступа к ресурсам на основе уровня секретности и целостности. В контексте Astra Linux мандатный контроль целостности осуществляется с помощью специальной подсистемы, называемой LSM (Linux Security Modules), которая позволяет определять и применять политики безопасности на уровне ядра операционной системы. Основные принципы мандатного контроля целостности Astra Linux: 1. Метки безопасности: Astra Linux использует метки безопасности для классификации объектов (файлов, процессов, ресурсов) и субъектов (пользователей, приложений) в соответствии с установленными правилами безопасности. 2. Правила доступа: Администраторы могут определять правила доступа на основе меток безопасности, задавая, кто и в каких условиях имеет право на чтение, запись или выполнение определенных ресурсов. 3. Целостность данных: Мандатный контроль целостности в Astra Linux обеспечивает защиту от несанкционированных изменений данных путем контроля и ограничения доступа к ним на основе уровня целостности. 4. Аудит: Astra Linux предоставляет возможность аудита действий пользователей и приложений, что позволяет отслеживать и анализировать события, связанные с доступом к ресурсам. Применение мандатного контроля целостности в Astra Linux способствует обеспечению высокого уровня безопасности операционной системы путем строгого контроля доступа к ресурсам на основе установленных правил безопасности и меток безопасности.