Федеральное государственное образовательное бюджетное

учреждение высшего образования

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

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По Учебной практике**

Дисциплина/Профессиональный модуль: Операционные системы

Выполнил студент

Группы:2ОИБАС-1222

Протасов Д.К.

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2024г.**

**Первая часть**

**Практическая работа №6. «Управление учетными записями пользователей»**

**Цель работы:** Сформировать навык студентов по созданию и управлению учетными записями пользователей.

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. В результате на экране откроется окно, изображенное на рис. 1.

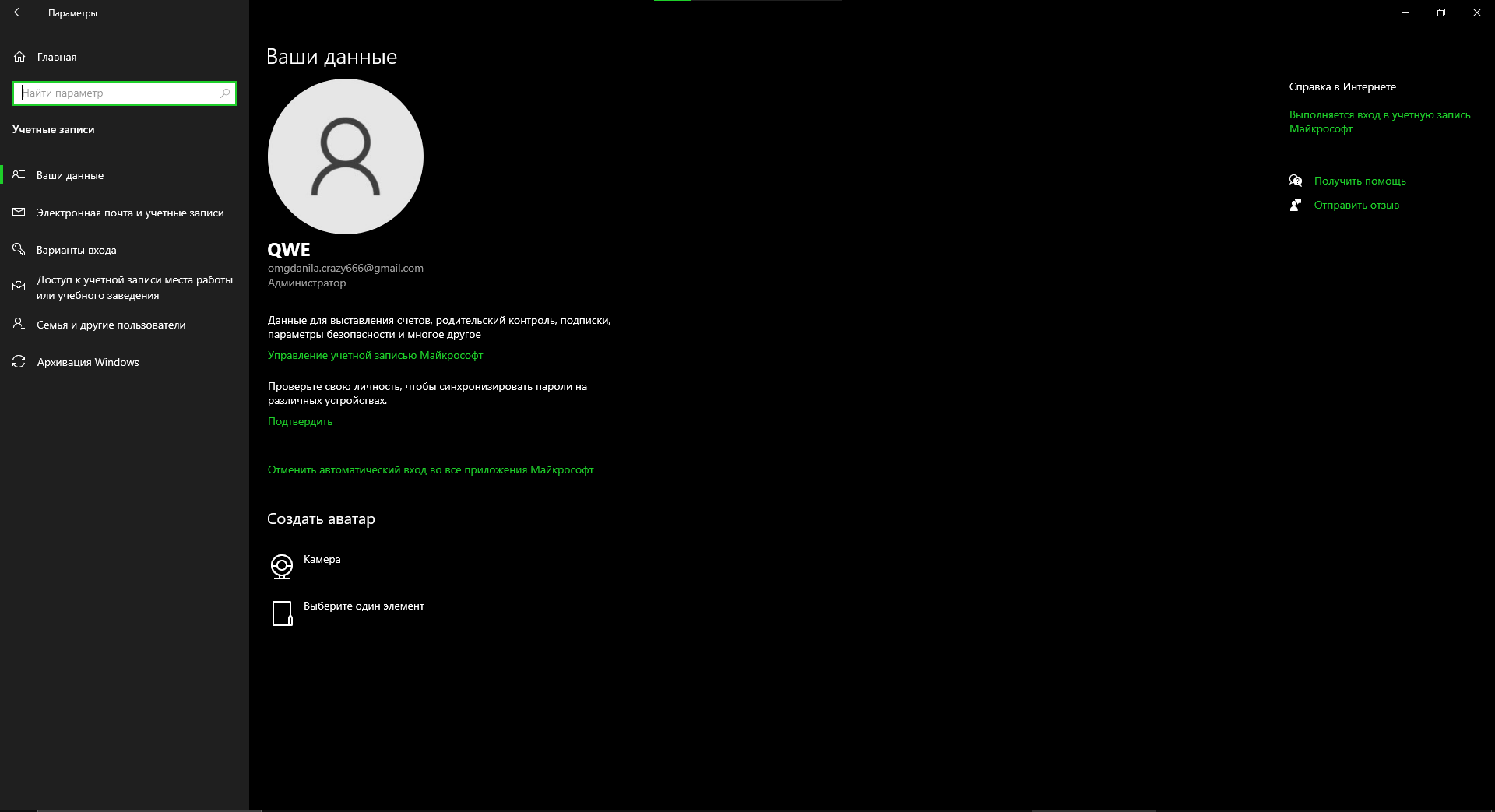


Рисунок 1

В данном окне содержится перечень созданных ранее учетных записей, а также меню Выберите задание. Вы можете самостоятельно создавать новые и редактировать имеющиеся записи, а также удалять их. Далее мы рассмотрим каждый из этих режимов.

**Ввод новой учетной записи**

Чтобы создать новую учетную запись, щелкните мышью на ссылке Создание учетной записи – при этом на экране отобразится окно, показанное на рис. 2.

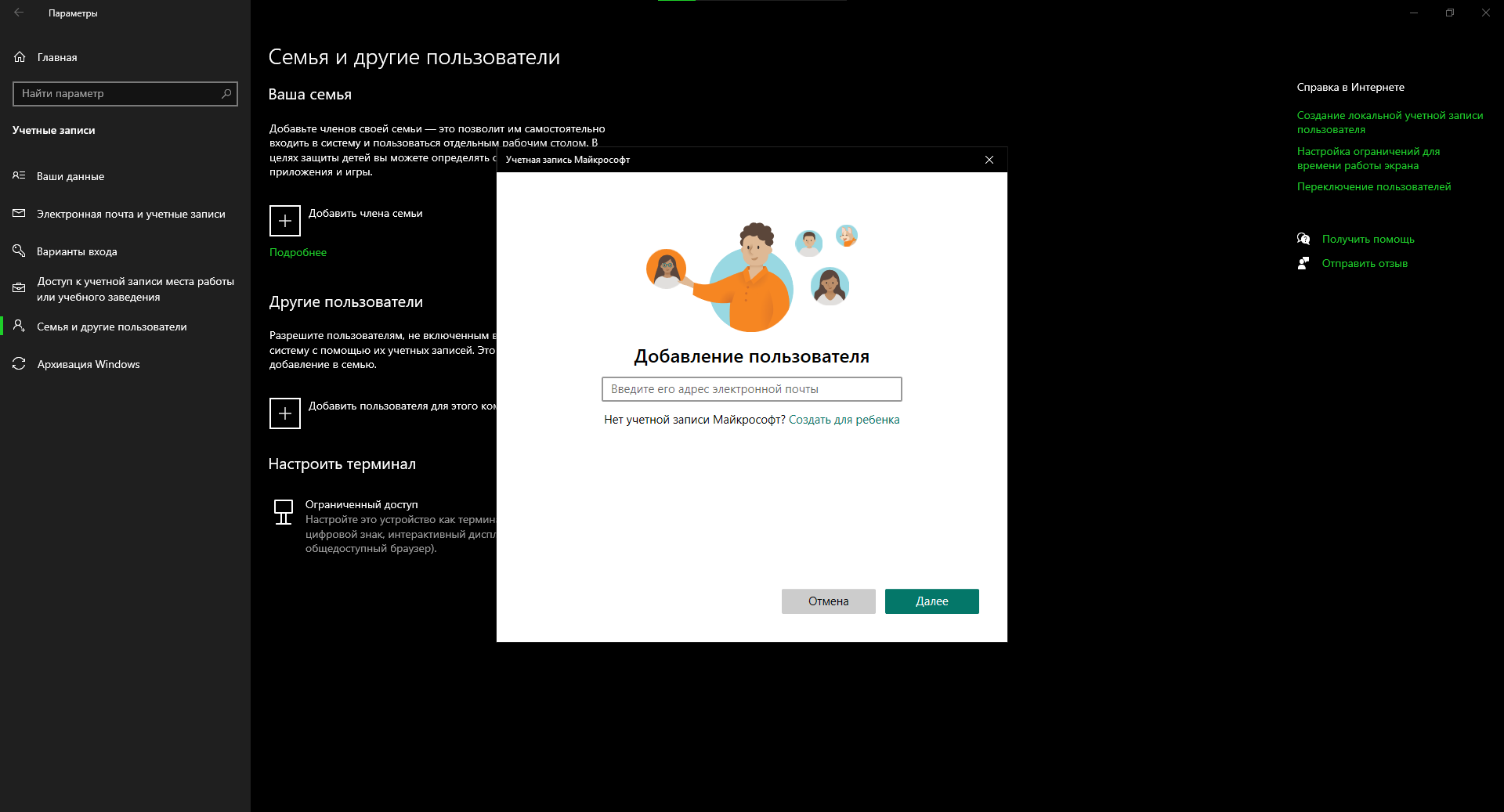
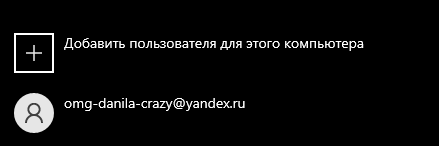


Рисунок 2

В данном окне необходимо с клавиатуры ввести имя создаваемой учетной записи. В качестве имени можно использовать любое слово, произвольный набор символов и т. д. Например, на рис. 3 созданным учетным записям присвоены имена Alex, Запись для сети, Администратор и Гость.

После этого с помощью соответствующего переключателя необходимо выбрать тип создаваемой учетной записи; возможные значения – Обычный доступ и Администратор (функциональные различия между типами учетных записей пользователей приведены выше).

Завершается процесс создания учетной записи пользователя нажатием кнопки Создание учетной записи – после этого новая учетная запись отобразится в списке учетных записей (рис. 3). Кнопка Отмена предназначена для выхода из данного режима без сохранения изменений.



**Редактирование и удаление учетных записей**

Для перехода в режим редактирования учетной записи необходимо щелкнуть мышью на ее значке. В результате в открывшемся окне будет выдан запрос на выполнение дальнейших действий; для выбора необходимо щелкнуть на одной из следующих ссылок:

• Изменение имени учетной записи;

• Создание пароля;

• Изменение рисунка;

• Установить родительский контроль;

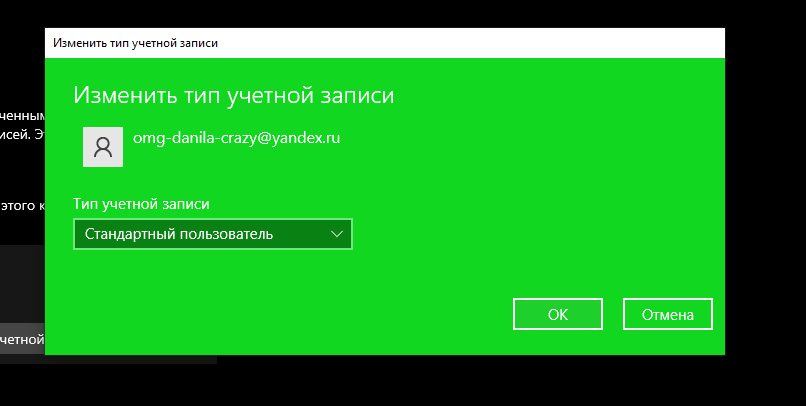
• Изменение типа учетной записи;

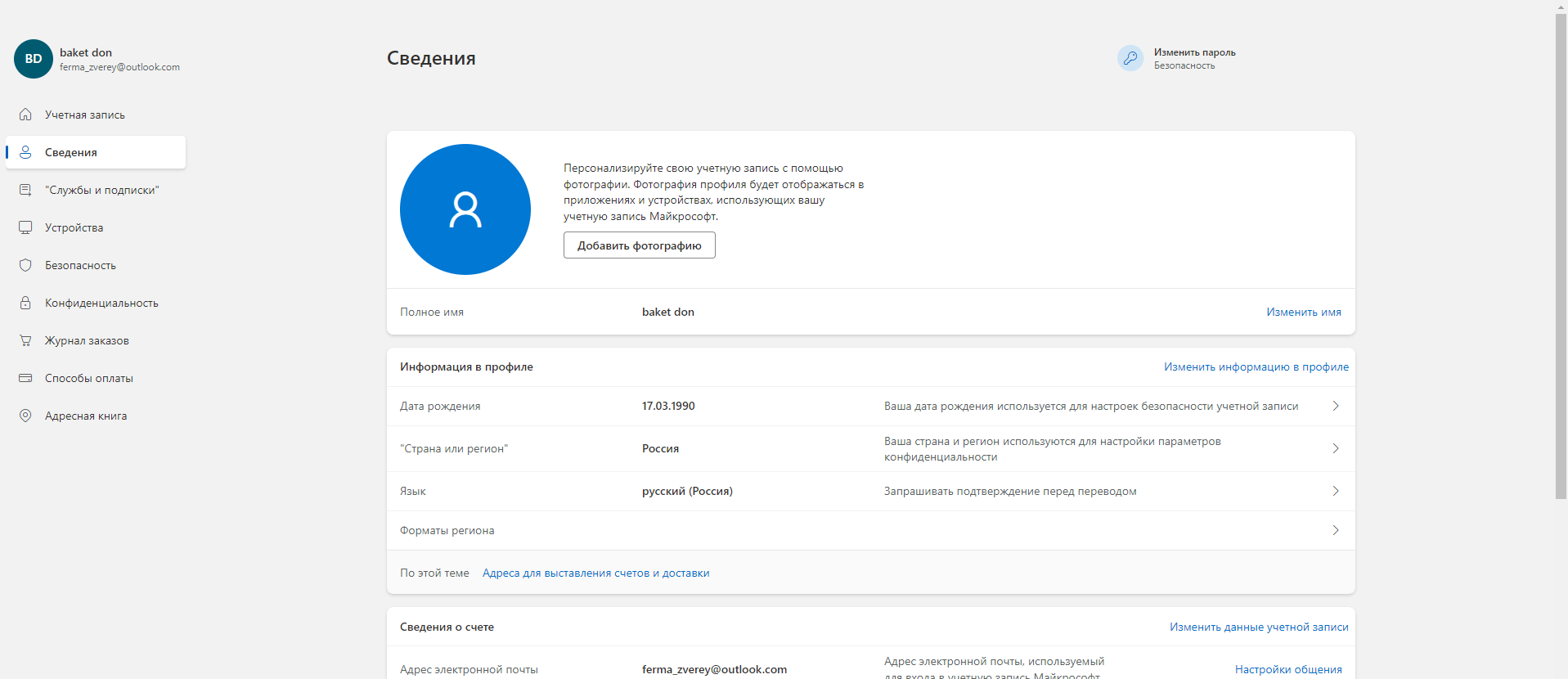
• Удаление учетной записи.

Если для выбранной учетной записи пароль был задан ранее, то вместо ссылки Создание пароля в списке будут присутствовать ссылки Изменение пароля и Удаление пароля.

При щелчке на ссылке Изменение имени учетной записи на экране откроется окно, похожее на окно, изображенное на рис. 5.2. Разница заключается в том, что в нем будет отсутствовать переключатель выбора типа учетной записи, а вместо кнопки Создание учетной записи находится кнопка Переименовать.

При выборе ссылки Создание пароля на экране откроется окно, которое показано на рис..4.





**Родительский контроль**

В любой семье, где есть несовершеннолетние дети, рано или поздно возникает проблема ограничения доступа ребенка к компьютеру. Не секрет, что в последние годы серьезно обострилась проблема компьютерной зависимости детей и подростков. Над этой проблемой работают психологи, педагоги и другие специалисты, и все они отмечают: компьютерная зависимость – это болезнь. Причем она влечет за собой возникновение еще целого ряда расстройств, которые в общем случае можно разделить на две категории: психические и физические.

Среди психических расстройств среди детей и подростков, возникновение которых обусловлено компьютерной зависимостью, можно отметить следующие:

• отсутствие интереса к «живому» общению и, напротив – чрезмерное увлечение виртуальным общением (электронная почта, чаты, и т. п.);

• неумение на словах выразить свои мысли;

• молчаливость, замкнутость;

• раздражительность;

• явное снижение интереса к окружающей действительности, стремление в любую свободную минуту сесть за компьютер;

• утомляемость, снижение успеваемости в школе, неумение сосредоточиться;

• нарушение сна;

• ухудшение аппетита.

Что касается физических расстройств у детей, страдающих компьютерной зависимостью, то среди них в первую очередь можно выделить:

• ухудшение зрения (несмотря на то, что жидкокристаллические мониторы считаются почти безвредными, глаза при работе за компьютером в любом случае находятся в напряжении, особенно при увлечении различными играми, «стрелялками», и т. п., не говоря уже об ЭЛТ – мониторах);

• изменение осанки вплоть до искривления позвоночника;

• головные боли;

• проблемы в области таза.

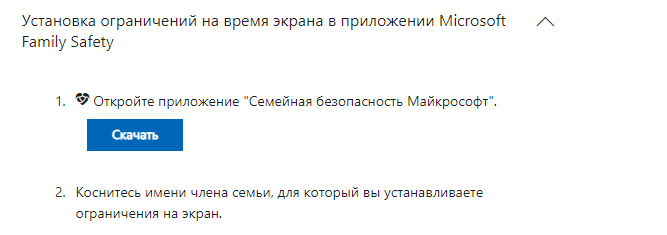
Но любое заболевание, как известно, легче предупредить, чем излечить. В данном разделе мы расскажем о том, как с помощью реализованной в Windows 7 функции родительского контроля ограничить использование ребенком компьютера (это касается как времени работы за компьютером, так и доступа к тем или иным приложениям и материалам).

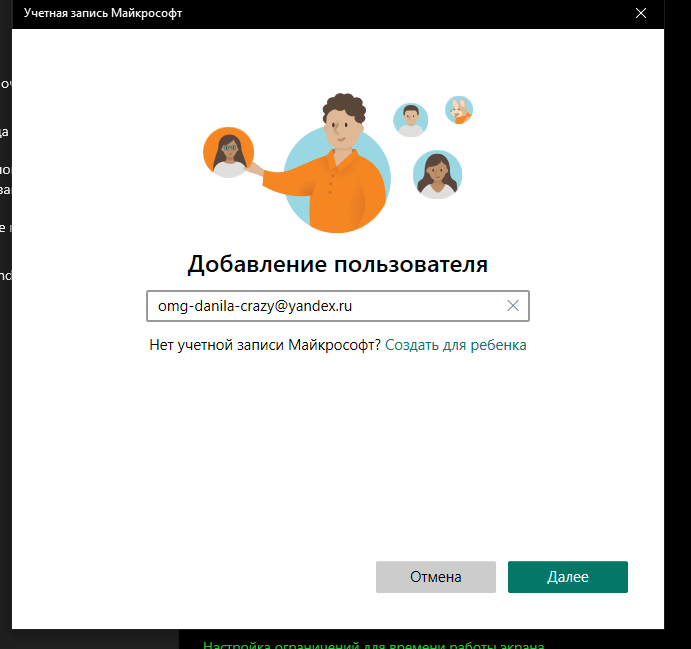
Родительский контроль позволяет регулировать использование компьютера детьми. В частности, можно определить промежутки времени, на протяжении которых дети могут работать за компьютером, а также установить, какими играми и приложениями они могут пользоваться.

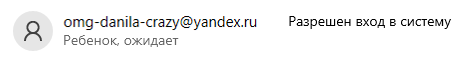
Если ребенок попытается запустить запрещенную игру или открыть запрещенную программу, то на экране отобразится информационное сообщение о том, что данное приложение заблокировано. В данном случае ребенок с помощью соответствующей ссылки может запросить разрешение на доступ к приложению, и вы можете предоставить этот доступ, указав свои учетные данные.

**Настройка ограничения времени работы за компьютером**

Чтобы ограничить время нахождения ребенка за компьютером, щелкните на ссылке Ограничение по времени (см. рис. 7). В результате на экране отобразится окно, изображенное на рис. 8.



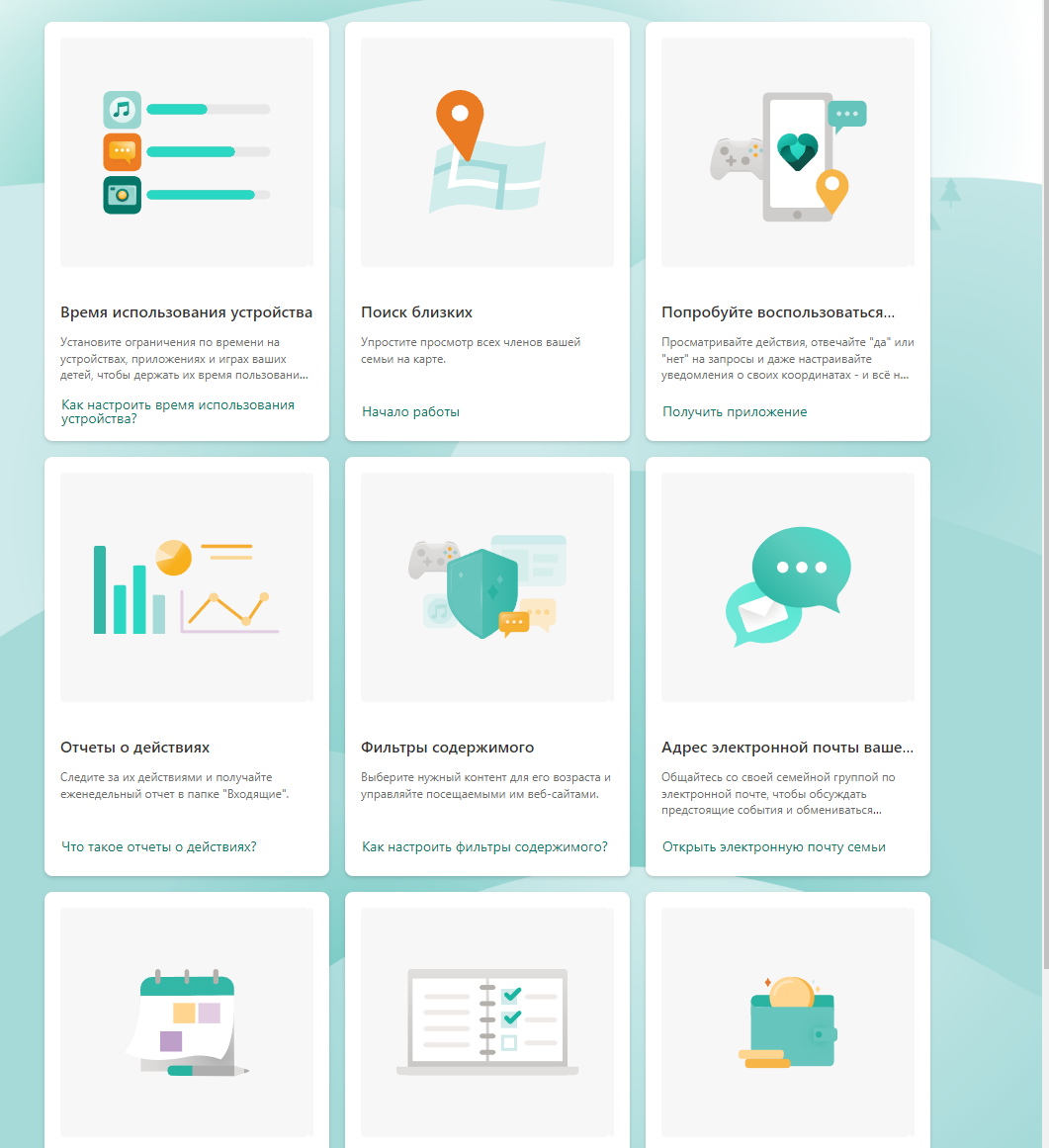




**Настройка ограничения доступа к играм**

В настоящее время на IT – рынке представлено великое множество самых разнообразных компьютерных игр. Среди них есть как полезные для детей и подростков игры, так и те, доступ к которым имеет смысл ограничить. Среди полезных компьютерных игр можно отметить, например, развивающие и обучающие игры, а среди вредных для детской психики – разные «стрелялки», игры со сценами насилия, интимных сцен, разжигающие национальную рознь, и т. д.

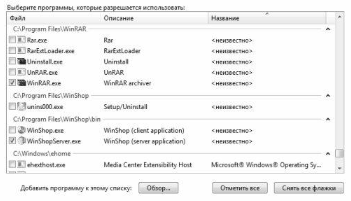
Чтобы ограничить доступ ребенка к установленным на компьютере играм, щелкните на ссылке Игры (см. рис. 7). В результате на экране откроется окно, изображенное на рис. 9.



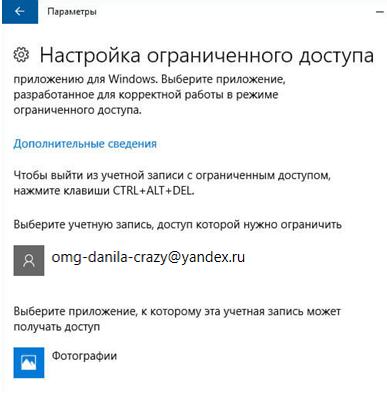
**Настройка ограничения доступа к приложениям**

Как мы уже отмечали ранее, вы можете настроить для вашего ребенка ограничение на доступ к имеющимся на компьютере программам. Это полезно нее только для того, чтобы запретить ребенку пользоваться сомнительными приложениями, но и с целью защиты своих данных от порчи или утраты. Например, если у вас хранится много важных данных в разных Excel – документах, то можно от греха подальше вообще заблокировать для ребенка запуск табличного редактора Excel. Как вариант – можно настроить ограничение прав доступа к конкретным файлам и папкам, но о том, как это делать, мы расскажем позже.

Чтобы ограничить доступ к установленным на компьютере приложениям, щелкните на ссылке Разрешение и блокировка отдельных программ (см. рис. 7). В результате на экране откроется окно, которое показано на рис. 11.



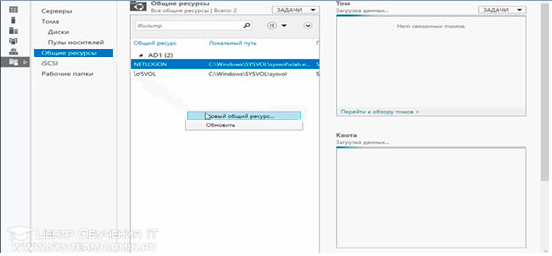
**Настройка ограничения доступа к приложениям**



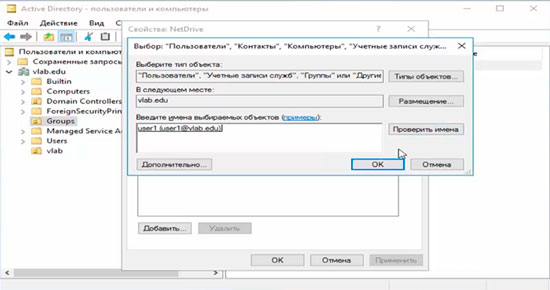
Вывод: научились манипулировать учетными записями в windows.

**Вторая часть**

Создаю общий ресурс на файловом сервере



Захожу в Диспетчер серверов, перехожу в раздел "Общие ресурсы", щелкаю правой кнопкой мыши и создаю ресурс. Оставляю параметры по умолчанию.



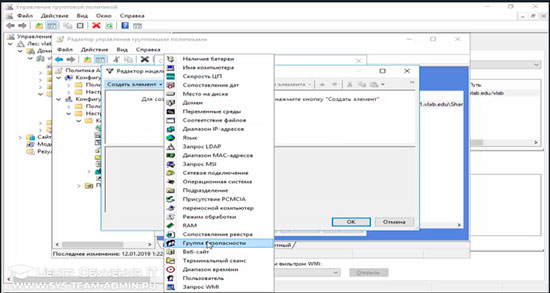
Создаю подразделение, пользователя и группу в Active Directory Windows Server 2016

Открываю оснастку "Пользователи и компьютеры", щелкаю правой кнопкой мыши на домене и создаю новое подразделение. Называю его "vlab".

В этом подразделении создаю нового пользователя "user1". Под ним буду входить в домен на клиентской машине.

В разделе групп создаю группу "NetDrive" и добавляю в нее пользователя "user1". Эта группа понадобится как фильтр безопасности для применения групповой политики.

Создаю и конфигурирую групповую политику Windows Server 2016



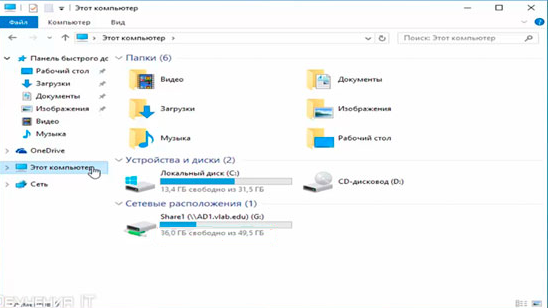
Открываю оснастку "Управление групповой политикой" и в разделе объектов создаю новую групповую политику. Называю ее "AddNetDrive".

Меняю содержимое групповой политики. В разделе конфигурации пользователя перехожу в раздел "Настройки", затем в "Конфигурация Windows" и выбираю "Сопоставление дисков".

Создаю элемент "Сопоставленный диск". В параметрах указываю путь к общему ресурсу (например, \\ad1\share), букву диска и устанавливаю флажок "Выполнять в контексте пользователя".

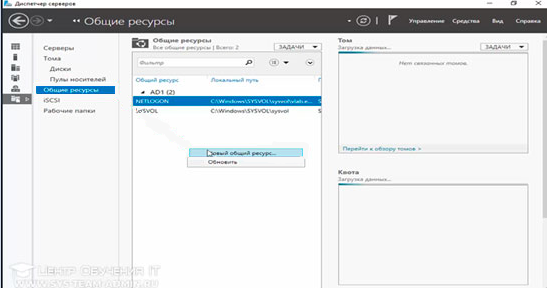
Привязываю объект к подразделению "vlab" и указываю в фильтре безопасности группу "NetDrive".

Вхожу в систему и проверяю подключение сетевого диска

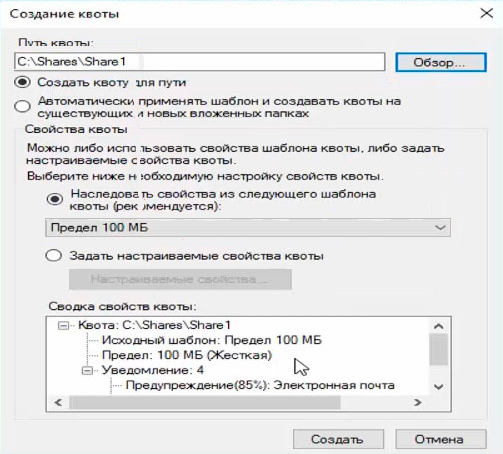


Ввожу учетные данные и вхожу в систему под доменной учетной записью "user1". Проверяю, подключился ли сетевой диск. Диск подключен.

Устанавливаю квоту на дисковое пространство

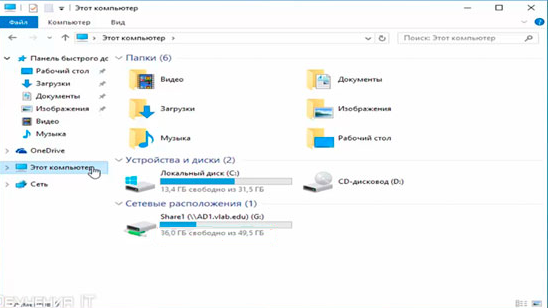


Открываю Диспетчер ресурсов файлового сервера, перехожу в раздел квот и создаю новую квоту. Назначаю ей параметры по умолчанию.



Этого достаточно, чтобы изучить принцип действия квотирования.

Проверяю применение квоты



Возвращаюсь на клиентский ПК и проверяю, что квота применена и функционирует. Доступное для использования пространство общего ресурса ограничено размером в 100 МБ. убери звездочки

**Третья часть**

**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.

**Задание на лабораторную работу**

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

**Порядок выполнения работы**

Создание учетной записи

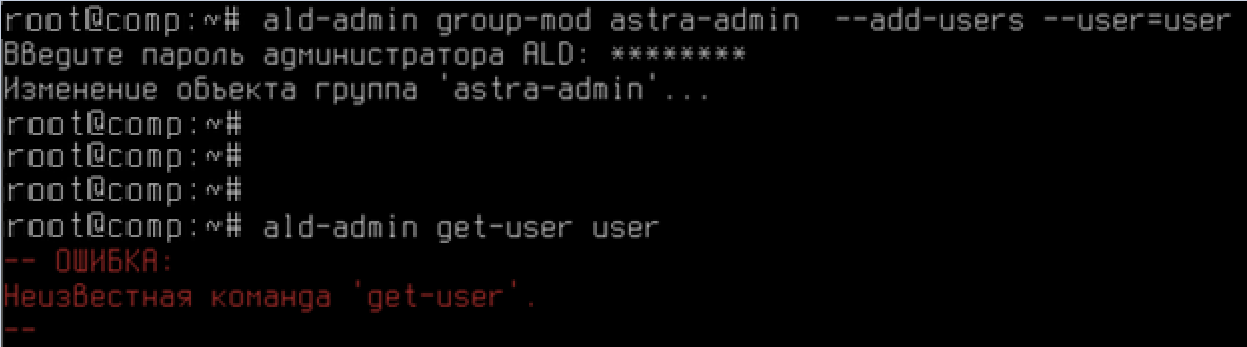


Рис. 1

Вход в учётную запись пользователя «user»



Рис. 2.

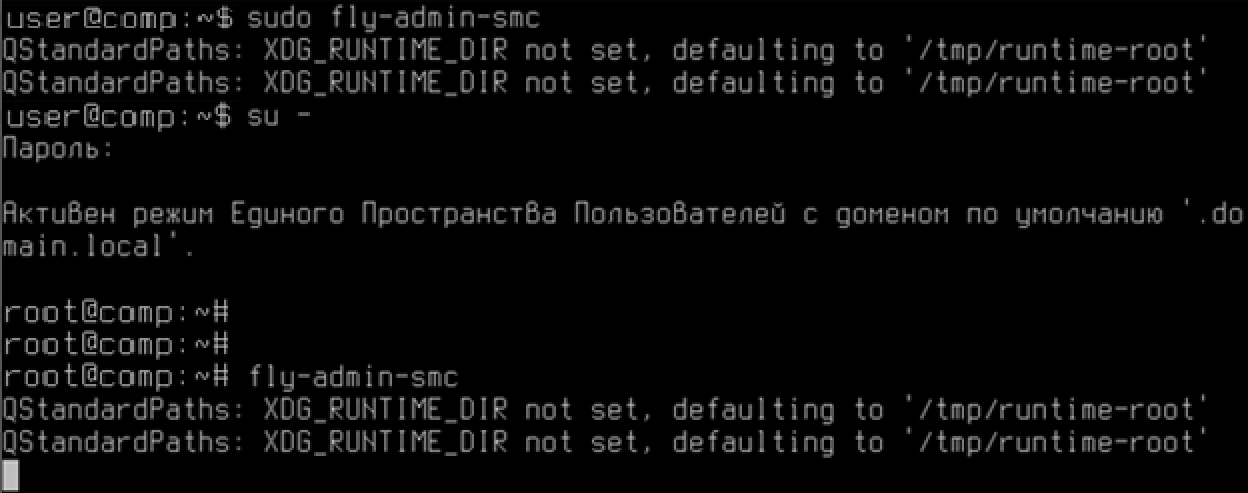
Запуск графической утилиты 

Рис. 3.

Создание уровней доступа 

Рис.4.

Создание пользователя user1 с уровнем доступа 4



Рис. 5.

Удаление уровня доступа 

Рис. 6.

Проверка отсутствия уровня 4

Рис. 7.

Создание новых учётных записей



Рис. 8.

* 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».

Пункты a-c

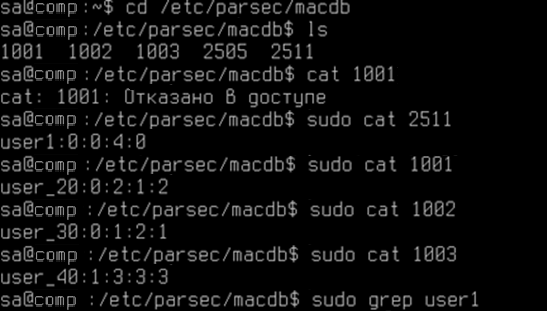


Рис. 9.

Пункты d-f

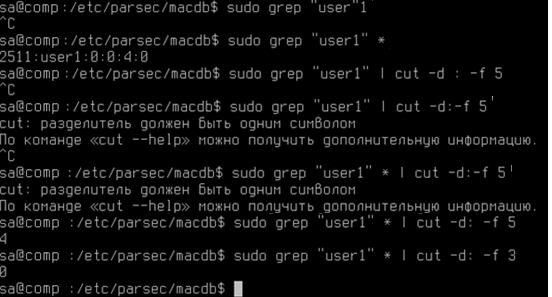


Рис. 10.

Проверка вывода команд на соответствие выводу графической утилиты



Рис. 11.

Создание новой иерархической категории



Рис. 12.

Ввод наименований



Рис. 13.

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».

Создание новой группы



Рис. 14.

Создание новой учётной записи



Рис. 15.

Выполнение пункта c



Рис. 16.

Выполнение пункта d



Рис. 17.

Структура каталогов 

Рис. 18.

1. 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*

Задание параметров мандатного и дискреционного управления доступом

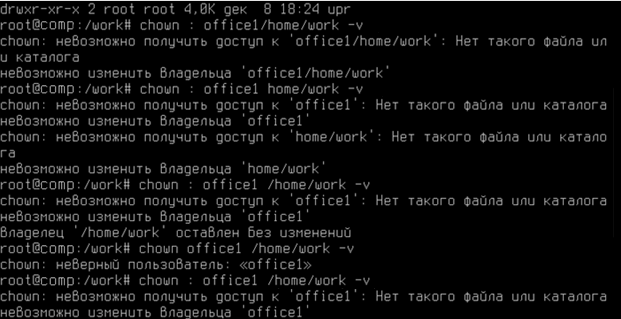


Рис. 19.

Листинг команд 14 пункта



Рис. 20.

Листинг команд 14 пункта (продолжение)



Рис. 21.

Листинг команд 14 пункта (продолжение) (продолжения)



Рис. 22.

Вывод

В ходе выполнения лабораторной работы была изучена мандатная система управления доступом Astra Linux к домену.

**Четвертая часть**

**Мандатный контроль целостности в Astra Linux 1.6**

**Введение**

Мандатный контроль целостности (МКЦ) - это мощный механизм безопасности, который защищает систему от несанкционированных изменений и эксплуатации уязвимостей.

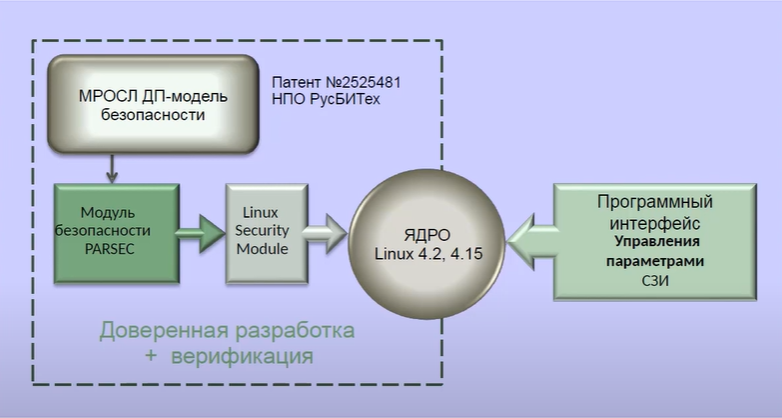
МКЦ реализован в Astra Linux 1.6 с помощью подсистемы безопасности Parsec.

**Теоретическое обоснование**

Дискреционное ограничение доступа (ДОС)\*\* контролирует доступ пользователей к файлам и другим ресурсам системы. Однако ДОС не позволяет управлять информационными потоками и предотвращать утечку данных.

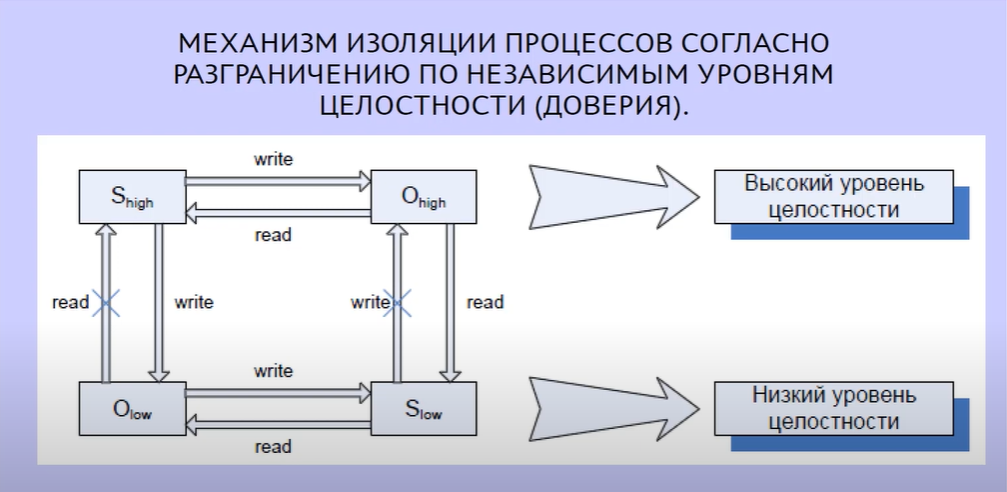
Мандатное управление доступом (МУД)\*\* вводит более детальные уровни контроля, основанные на уровнях конфиденциальности и категориях. МКЦ является частью МУД и дополняет его.

**Как работает МКЦ**



МКЦ использует концепцию уровней целостности. Объектам в системе (файлам, процессам и т.д.) присваиваются уровни целостности, которые определяют их важность для функционирования системы.

МКЦ не позволяет процессам с более низким уровнем целостности модифицировать объекты с более высоким уровнем целостности. Это предотвращает эксплуатацию уязвимостей в приложениях с более высоким уровнем целостности.



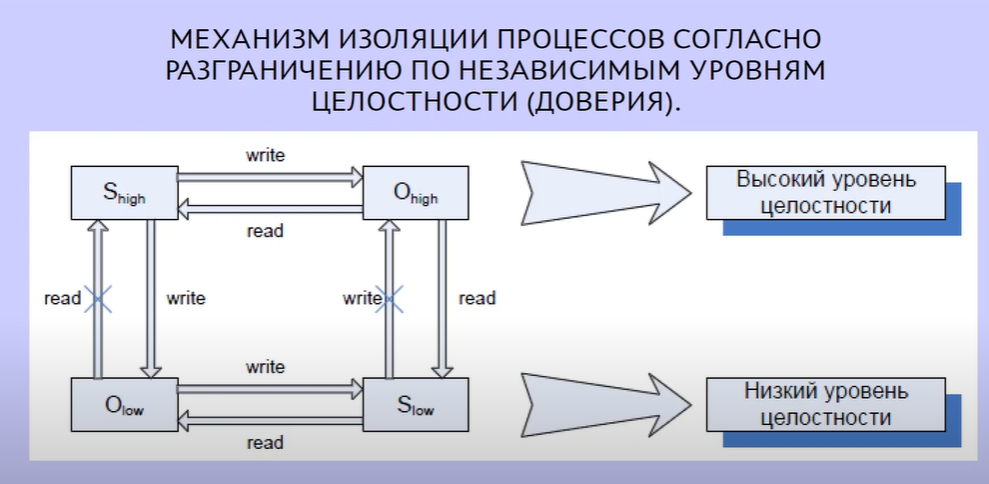
**Реализация в Astra Linux 1.6**

****

В Astra Linux 1.6 МКЦ используется для защиты приложений и их конфигурационных файлов.

Файлы изначально имеют максимальный уровень целостности.

Для включения МКЦ необходимо активировать защиту файловой системы в панели управления.



**Преимущества МКЦ**

Усложняет эксплуатацию уязвимостей нулевого дня.

Повышает безопасность системы путем управления информационными потоками.

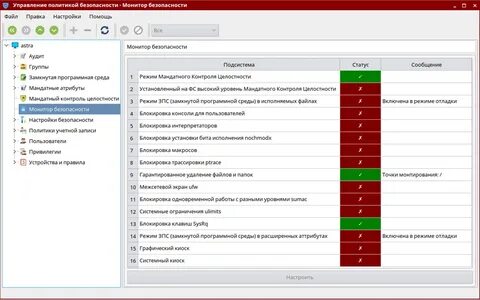
Усложняет проведение атак через взлом приложений.

**Мониторинг и защита от эксплоитов**



Монитор Parsec отслеживает действия процессов с низким уровнем целостности. Если обнаруживается попытка создания или запуска процесса с высоким уровнем целостности, Parsec прибивает такой процесс.

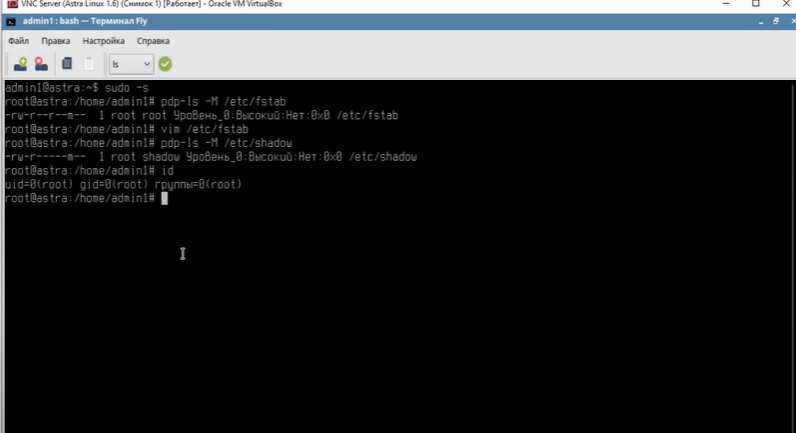
**Примеры работы МКЦ**



В Windows процессы с низким уровнем целостности не могут влиять на процессы с высоким уровнем, даже если они получают привилегии администратора.

В Astra Linux МКЦ защищает системные файлы и приложения от модификации неавторизованными пользователями или вредоносным ПО.

**Активация МКЦ**

****

Для активации МКЦ необходимо зайти в панель управления и включить защиту файловой системы.

После этого все файлы получат максимальный уровень контроля целостности.

**Ограничения МКЦ**

МКЦ не применяется к памяти и оперативной памяти.

Для внесения изменений в файлы с высоким уровнем целостности необходимо войти под соответствующим уровнем.

**Настройка МКЦ**

Уровни целостности и политики МКЦ можно настроить с помощью специальных утилит.

Рекомендации по настройке зависят от конкретной системы и приложений.

**Заключение**

МКЦ является важным инструментом защиты Astra Linux 1.6 от эксплойтов и несанкционированных изменений. Его использование значительно повышает уровень безопасности системы, делая ее устойчивой к различным атакам.