**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Программно-аппаратные средства защиты информации»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

«ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ВИРТУАЛИЗАЦИИ»

**Выполнили:**

Ахраров Али Рустамович, студент группы N3250

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Калабишка Михаил Михайлович

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Оглавление

[Введение 4](#_Toc182431427)

[2 Ход работы 5](#_Toc182431428)

[2.1 Выбор дистрибутива и системы 5](#_Toc182431429)

[2.2 Нормативная база 5](#_Toc182431430)

[3 Настройка системы защиты 6](#_Toc182431431)

[3.1 Идентификация и аутентификация пользователей 6](#_Toc182431432)

[3.2 Управление доступом к объектам 6](#_Toc182431433)

[3.3 Защита машинных носителей персональных данных 7](#_Toc182431434)

[3.4 Регистрация событий безопасности 7](#_Toc182431435)

[3.5 Антивирусная защита 7](#_Toc182431436)

[3.6 Управление конфигурацией информационной системы 8](#_Toc182431437)

[4 Заключение 9](#_Toc182431438)

Введение

Цель: ознакомление с базовыми модулями защиты Unix систем

Задачи:

* Предопределить дистрибутив(смотрим в список)
* Определить в какой системе расположен защищаемый эндпоинт
* Предопределить требования к защите с помощью нормативной базы
* Выполнить настройку Unix системы в соответствии с требованиями
* Регуляторов

# Ход работы

## Выбор дистрибутива и системы

Для выполнения данной лабораторной работы в качестве операционной системы выбран **openSuse**. Тип защищаемой информационной системы **— автоматизированная система класса 3А (АС 3А).**

## Нормативная база

Классификация автоматизированных систем (АС) по защищенности от несанкционированного доступа (НСД) к информации в России регулируется руководящим документом **«Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»**, утвержденным Государственной технической комиссией при Президенте РФ 30 марта 1992 года.

Согласно этому документу, АС подразделяются на три группы, каждая из которых включает несколько классов защищенности:

1. **Первая группа**: многопользовательские АС, обрабатывающие информацию разных уровней конфиденциальности, при этом не все пользователи имеют равные права доступа. Включает классы **1Д, 1Г, 1В, 1Б и 1А**.
2. **Вторая группа**: АС, в которых пользователи имеют одинаковые полномочия доступа ко всей информации, обрабатываемой и хранимой на носителях различного уровня конфиденциальности. Включает классы **2Б и 2А**.
3. **Третья группа**: АС, в которых работает один пользователь, допущенный ко всей информации, размещенной на носителях одного уровня конфиденциальности. Включает классы **3Б и 3А**.

Класс **3А** относится к третьей группе и характеризуется следующими признаками:

* **Количество пользователей**: один пользователь.
* **Уровень конфиденциальности информации**: вся информация имеет один уровень конфиденциальности.
* **Полномочия доступа**: пользователь имеет полный доступ ко всей информации в системе.

Для АС класса 3А устанавливаются минимальные требования по защите информации от НСД, поскольку в таких системах отсутствует необходимость разграничения прав доступа между пользователями.

Таким образом, нормативная база для АС класса 3А определяется вышеуказанным руководящим документом, который устанавливает классификацию АС и соответствующие требования по защите информации от несанкционированного доступа

**Требования к классу защищенности 3А:**

Подсистема управления доступом:

должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова.

Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

- результат попытки входа: успешная или неуспешная (при НСД);

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);

- краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;

- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

- должно проводиться несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Подсистема обеспечения целостности:

должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

- должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

|  |  |  |
| --- | --- | --- |
| **Подсистемы и требования** | **Классы** | |
| **3Б** | **3А** |
| 1. Подсистема управления доступом |  |  |
| 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: |  |  |
| в систему | + | + |
| к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ | - | - |
| к программам | - | - |
| к томам, каталогам, файлам, записям, полям записей | - | - |
| 1.2. Управление потоками информации |  |  |
| 2. Подсистема регистрации и учета |  |  |
| 2.1. Регистрация и учет: |  |  |
| входа (выхода) субъектов доступа в (из) систему(ы) (узел сети) | + | + |
| выдачи печатных (графических) выходных документов | - | + |
| запуска (завершения) программ и процессов (заданий, задач) | - | - |
| доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи | - | - |
| доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей | - | - |
| изменения полномочий субъектов доступа | - | - |
| создаваемых защищаемых объектов доступа | - | - |
| 2.2. Учет носителей информации | + | + |
| 2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей | - | + |
| 2.4. Сигнализация попыток нарушения защиты | - | - |
| 3. Криптографическая подсистема |  |  |
| 3.1. Шифрование конфиденциальной информации | - | - |
| 3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах | - | - |
| 3.3. Использование аттестованных (сертифицированных) криптографических средств | - | - |
| 4. Подсистема обеспечения целостности |  |  |
| 4.1. Обеспечение целостности программных средств и обрабатываемой информации | + | + |
| 4.2. Физическая охрана средств вычислительной техники и носителей информации | + | + |
| 4.3. Наличие администратора (службы) защиты информации в АС | - | - |
| 4.4. Периодическое тестирование СЗИ НСД | + | + |
| 4.5. Наличие средств восстановления СЗИ НСД | + | + |
| 4.6. Использование сертифицированных средств защиты | - | + |

# Настройка системы защиты

## Идентификация и аутентификация пользователей

1. **Создание учетных записей пользователей**:
   * Используйте команду useradd для создания новых пользователей или графические инструменты openSuse.
   * Пароли устанавливаются командой passwd.
   * Информация о пользователях хранится в /etc/passwd, пароли в /etc/shadow (этот файл защищен от несанкционированного доступа).
2. **Многофакторная аутентификация:**
   * Для дополнительной безопасности можно настроить многофакторную аутентификацию с помощью **PAM** модулей, а также USB-ключи для второго фактора.
3. **Управление идентификаторами**:
   * Для управления идентификаторами пользователей используйте команды adduser, usermod для назначения уникальных идентификаторов и команду deluser для удаления пользователей.
   * Для обеспечения надежного хранения аутентификационной информации используется файл /etc/shadow.

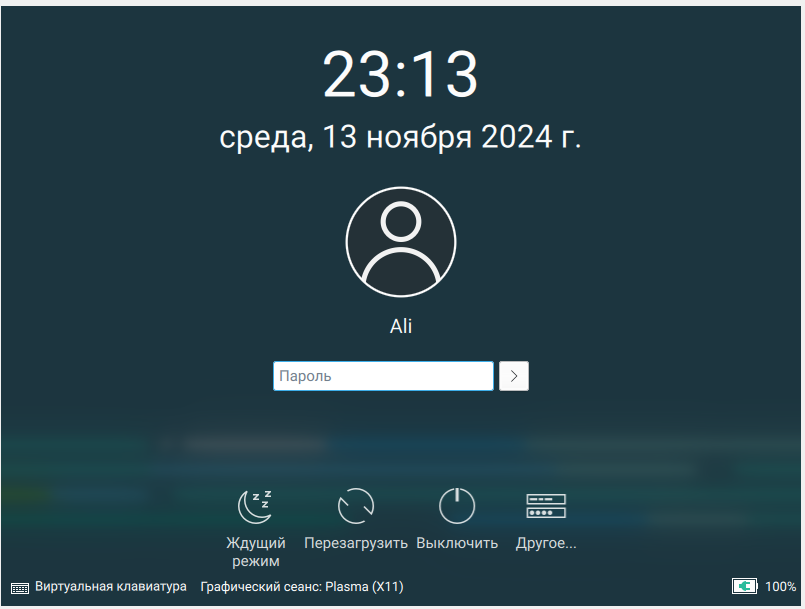


Рисунок 1 – Авторизация пользователя

## Управление доступом к объектам

1. **Настройка прав доступа к файлам и каталогам:**
   * Используйте команду chmod для настройки прав доступа, например: chmod 700 <имя\_файла> для полного доступа только владельцу.
   * Управление пользователями и группами можно выполнить с помощью usermod, addgroup, delgroup и других команд.
2. **Использование AppArmor и SELinux:**
   * Для обеспечения мандатного разграничения доступа и защиты приложений используется **AppArmor**, который ограничивает права доступа для приложений.
   * **SELinux** также можно использовать для обеспечения ролевой модели доступа.
3. **Маршрутизация и контроль сетевых потоков:**
   * Для фильтрации сетевого трафика используйте **iptables** для настройки межсетевого экрана. Например, добавление правила: iptables -A INPUT -p tcp --dport 22 -j ACCEPT для разрешения подключения по SSH.
4. **Разделение полномочий пользователей:**
   * Разделите полномочия между пользователями, администраторами и операторами, создав разные группы с разными уровнями привилегий. Например, используйте команду addgroup admin для создания группы администраторов и назначьте пользователей, которые будут выполнять административные функции.
   * Используйте команду usermod -aG <группа> <имя\_пользователя> для добавления пользователей в нужные группы.
5. **Минимально необходимые права:**
   * Используйте принцип минимально необходимых прав для всех пользователей и администраторов, предоставляя им доступ только к тем ресурсам, которые необходимы для выполнения их задач.

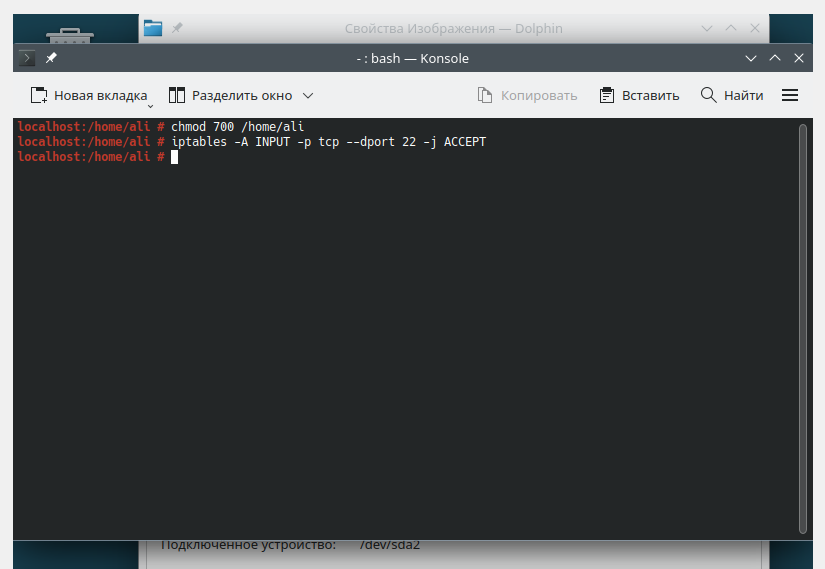


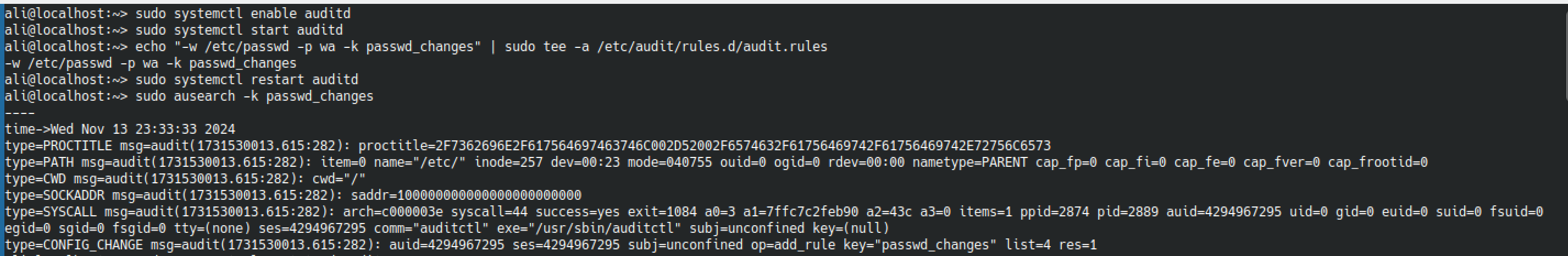
Рисунок 2 – использование команд «chmod» и «iptable»

## Защита машинных носителей персональных данных

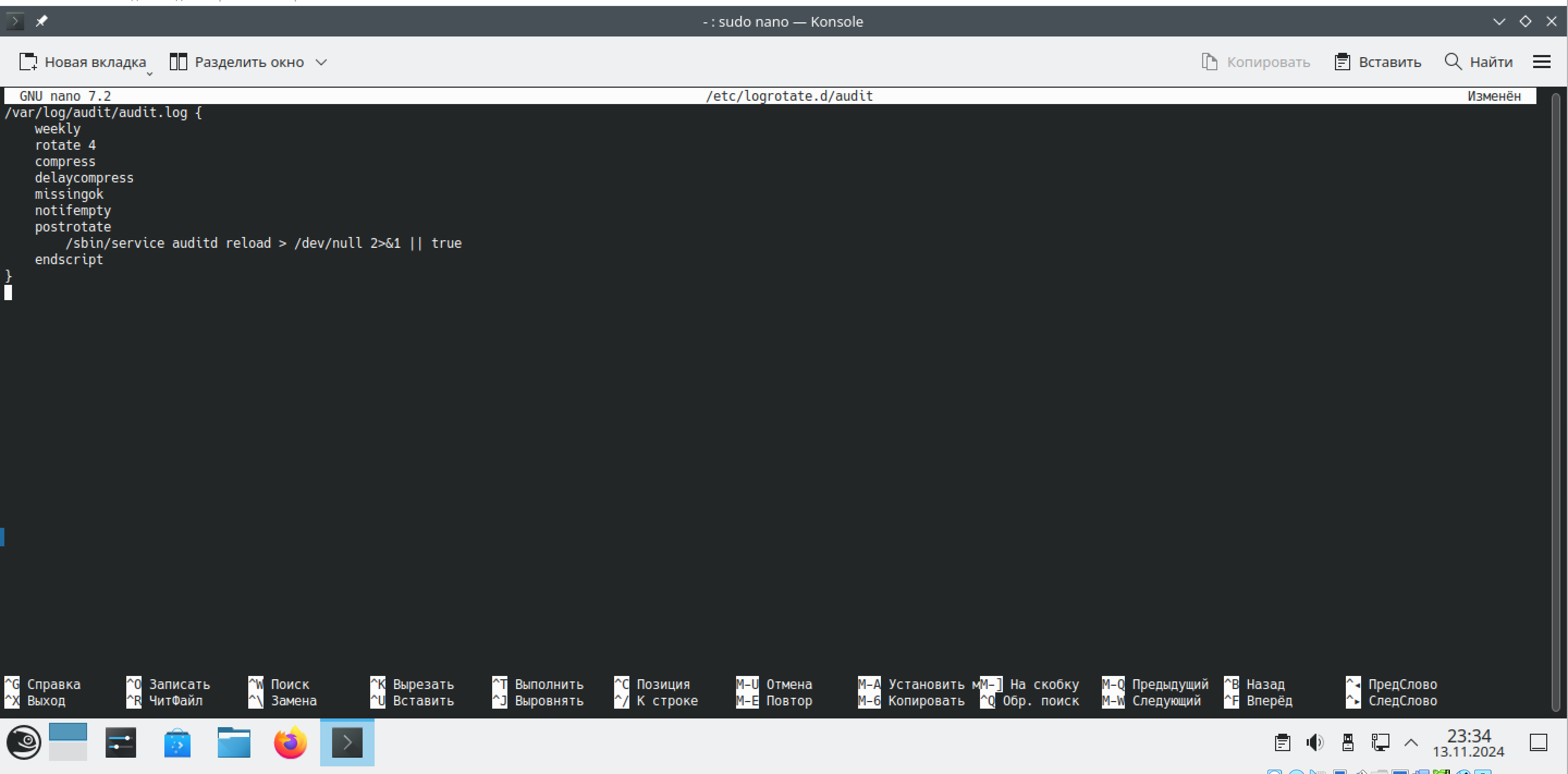
1. **Удаление данных:**
   * Для безопасного удаления данных используйте команду shred, которая перезаписывает данные несколько раз. Например: shred -u -n 5 <имя\_файла>.
   * Используйте также утилиты wipe и dd для полного стирания данных с жестких дисков.
2. **Контроль доступа к носителям**:
   * Для защиты машинных носителей используйте шифрование данных с помощью утилиты **LUKS**. Это обеспечит безопасность при утере или компрометации носителей.

## Регистрация событий безопасности

1. **Журналирование событий:**
   * В openSuse используется утилита **auditd** для регистрации действий пользователей и администраторов. Настройте ее для отслеживания важных действий, таких как попытки изменения конфигурации системы или доступ к конфиденциальным файлам.



* + Для архивирования логов используйте **logrotate** для автоматического управления старыми логами и удаления устаревших данных.





1. **Мониторинг изменений**:
   * Используйте утилиту **inotify** для отслеживания изменений в критически важных файлах и каталогах системы.
   * Настройте уведомления о несанкционированных попытках доступа или изменения важных файлов.
2. **Защита журналов событий:**
   * Ограничьте доступ к логам только администраторам с помощью настроек прав доступа chmod и chown.
   * Настройте передачу логов на удаленный сервер для дополнительной защиты и предотвращения манипуляций.

## Антивирусная защита

1. **Установка антивируса:**
   * Установите **ClamAV** для сканирования файлов на наличие вредоносного ПО. Используйте команду freshclam для обновления базы данных вирусов.
   * Настройте регулярное сканирование системы на наличие вирусов, используя **cron** задачи.
2. **Обновление антивирусных баз**:
   * Регулярное обновление баз данных вирусов — важная часть обеспечения безопасности. Настройте автоматическое обновление с помощью freshclam, чтобы всегда использовать актуальные версии.

## Управление конфигурацией информационной системы-

1. **Анализ и управление изменениями конфигурации:**
   * Конфигурация системы управляется через утилиту **YaST**. Через нее можно управлять разными аспектами системы, включая безопасность.
   * Все изменения конфигурации должны документироваться, чтобы отслеживать их влияние на систему безопасности.
   * Настройте утилиту **etckeeper** для контроля изменений в файлах конфигурации. Она использует систему контроля версий (например, **git**) для отслеживания всех изменений конфигурации в /etc.
2. **Назначение ответственных за изменения конфигурации:**
   * Определите список лиц, которым разрешено вносить изменения в конфигурацию системы и системы защиты данных.
   * Обеспечьте документирование всех внесенных изменений и контроль за их реализацией.

# Заключение

В ходе работы была выполнена настройка системы **openSuse** в соответствии с требованиями регуляторов для класса безопасности **АС 3А**. Были настроены идентификация и аутентификация пользователей, управление доступом, антивирусная защита, контроль событий и управление конфигурацией системы. Эти меры обеспечивают необходимый уровень защиты для автоматизированной системы класса АС 3А, согласно нормативным требованиям.