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

«Механизмы защиты Unix систем»

Выполнили:

Суханкулиев Мухаммет,

студент группы N3346

_____
(подпись)

Бардышев Артём Антонович,

студент группы N3346

_____
(подпись)

Проверил:

Чешев Никита Игоревич

_____
(отметка о выполнении)

_____
(подпись)

Санкт-Петербург

2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы – ознакомление с базовыми модулями защиты Unix систем.

Для достижения поставленной цели необходимо решить следующие задачи:

- Предопределить дистрибутив;
- Определить в какой системе расположен защищаемый эндпоинт;
- Предопределить требования к защите с помощью нормативной базы;
- Выполнить настройку Unix системы в соответствии с требованиями регуляторов.

1 LINUX MINT

1.1 Предопределить дистрибутив

В качестве операционной системы используется **Linux Mint**, дистрибутив семейства **Debian-based**. Данная принадлежность определяет ключевой стек технологий для обеспечения безопасности: для установки и обновления пакетов применяется `apt`, для фильтрации сетевого трафика – `ufw`, а для реализации мандатного контроля доступа – `AppArmor`.

1.2 Определить в какой системе расположен защищаемый эндпоинт

Защищаемый эндпоинт функционирует в составе информационной системы (ИС), которая обрабатывает **коммерческую тайну** (согласно ФЗ-98 "О коммерческой тайне") и классифицируется как **автоматизированная система (АС) класса 1В** (согласно РД ФСТЭК п 1.9).

Класс 1В подразумевает, что ИС является **многопользовательской**, где сотрудники с разными правами доступа работают с информацией различной степени конфиденциальности. Ключевым требованием к такой системе является **принудительное разграничение доступа** и контроль информационных потоков.

1.3 Предопределить требования к защите с помощью нормативной базы

Основным документом, диктующим технические требования, для нас будет **РД ФСТЭК по АС**. Мы откроем его и выпишем все требования, помеченные знаком "+" для класса **1В**.

На основе анализа РД ФСТЭК для АС класса 1В, сформирован следующий профиль защиты:

Таблица 1 – Требования (Linux Mint)

Требование из РД ФСТЭК (п. 2.13)	**Техническая мера защиты**	**Инструмент в Linux Mint**
1. Подсистема управления доступом		
1.1. Идентификация и аутентификация	Надежная парольная политика	Модуль PAM (`libpam-pwquality`)

1.1. Контроль доступа (дискреционный)	Разграничение прав на файлы/каталоги	Стандартные права POSIX (`chmod, chown`)
1.3. Управление потоками информации	Мандатный контроль доступа (MAC)	`AppArmor`
2. Подсистема регистрации и учета		
2.1. Регистрация входа/выхода, доступа к файлам, запуска программ	Ведение журналов аудита (логов)	Демон аудита (`auditd`)
2.2. Очистка областей ОЗУ и дисков	Гарантированное удаление данных	Встроенные механизмы ядра, утилиты
2.3. Сигнализация о попытках НСД	Оповещение администратора	Настройки `auditd, Fail2Ban`
3. Подсистема обеспечения целостности		
4.1. Целостность ПО и информации	Контроль неизменности системных файлов	Система обнаружения вторжений `AIDE`
4.2. Физическая охрана	(Организационная мера, не реализуется в ВМ)	-
4.3. Наличие администратора защиты	Создание отдельной роли администратора	Управление пользователями и `sudo`
4.4. Периодическое тестирование СЗИ	Проверка конфигурации и целостности	Скрипты, ручной запуск `aide –check`
4.6. Использование сертифицированных СЗИ	(Для лаб. работы имитируется настройкой)	-
Дополнительные меры (из КТ и общих практик)		
-	Шифрование данных при хранении	`LUKS` (при установке системы)
-	Межсетевое экранирование	`UFW` (Uncomplicated Firewall)
-	Своевременное обновление	`apt, unattended-upgrades`

1.4 Выполнить настройку Unix системы в соответствии с требованиями регуляторов

1.4.1 Начальная подготовка и обновления

```
# Обновляем списки пакетов
sudo apt update

# Устанавливаем все доступные обновления
sudo apt upgrade -y
```

Настроим автоматическую установку обновлений безопасности.

```
# Устанавливаем пакет
sudo apt install unattended-upgrades -y

# Запускаем мастер настройки
sudo dpkg-reconfigure --priority=low unattended-upgrades
```

```
mint@mint:~$ sudo apt upgrade -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  libllvm20
The following packages will be upgraded:
  bind9-dnsutils bind9-host bind9-libs coreutils cups cups-bsd cups-client cups-common cups-core-drivers cups-daemon cups-ipp-utils cups-ppdc
  cups-server-common firefox firefox-locale-de firefox-locale-en firefox-locale-es firefox-locale-fr firefox-locale-it firefox-locale-nl
  firefox-locale-pt firefox-locale-ru fwupd gir1.2-udisks-2.0 libadwaita-1-0 libcups2t64 libcupsimage2t64 libegl-mesa0 libfwupd2 libgbm1
  libgl1-mesa-dri libglx-mesa0 libudisks2-0 libxatracker2 libxml2 linux-firmware mesa-libgallium mesa-va-drivers mesa-vdpau-drivers
  mesa-vulkan-drivers mint-upgrade-info mintdrivers mintupdate openssh-client udisks2
45 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 701 MB of archives.
After this operation, 144 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 coreutils amd64 9.4-3ubuntu6.1 [1413 kB]
Get:2 http://packages.linuxmint.com zara/upstream amd64 firefox amd64 142.0.1+linuxmint1+zara [85.9 MB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libcupsimage2t64 amd64 2.4.7-1.2ubuntu7.4 [6662 B]
Get:4 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 cups-ipp-utils amd64 2.4.7-1.2ubuntu7.4 [233 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 cups-core-drivers amd64 2.4.7-1.2ubuntu7.4 [29.5 kB]
```

...

```
Updating PPD files for gutenprint ...
Updating PPD files for hpcups ...
Updating PPD files for m2300w ...
Updating PPD files for postscript-hp ...
Updating PPD files for ptouch ...
Updating PPD files for pxljr ...
Updating PPD files for sag-gdi ...
Updating PPD files for splix ...
Setting up libgbm1:amd64 (25.0.7-0ubuntu0.24.04.2) ...
Setting up cups-bsd (2.4.7-1.2ubuntu7.4) ...
Setting up libgl1-mesa-dri:amd64 (25.0.7-0ubuntu0.24.04.2) ...
Setting up libxatracker2:amd64 (25.0.7-0ubuntu0.24.04.2) ...
Setting up libegl-mesa0:amd64 (25.0.7-0ubuntu0.24.04.2) ...
Setting up bind9-dnsutils (1:9.18.39-0ubuntu0.24.04.1) ...
Setting up mesa-va-drivers:amd64 (25.0.7-0ubuntu0.24.04.2) ...
Setting up libglx-mesa0:amd64 (25.0.7-0ubuntu0.24.04.2) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1.1ubuntu3) ...
Processing triggers for libc-bin (2.39-0ubuntu8.5) ...
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libglib2.0-0t64:amd64 (2.80.0-6ubuntu3.4) ...
Processing triggers for dbus (1.14.10-4ubuntu4.1) ...
Processing triggers for mintsystem (8.6.3) ...
Processing triggers for install-info (7.1-3build2) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for desktop-file-utils (0.27-2build1) ...
Processing triggers for initramfs-tools (0.142ubuntu25.5) ...
```

Рисунок 1 – Скриншот выполнения `sudo apt upgrade`

1.4.2 Настройка подсистемы управления доступом

```
# Устанавливаем библиотеку
sudo apt install libpam-pwquality -y
# Открываем файл в текстовом редакторе
sudo nano /etc/security/pwquality.conf
```

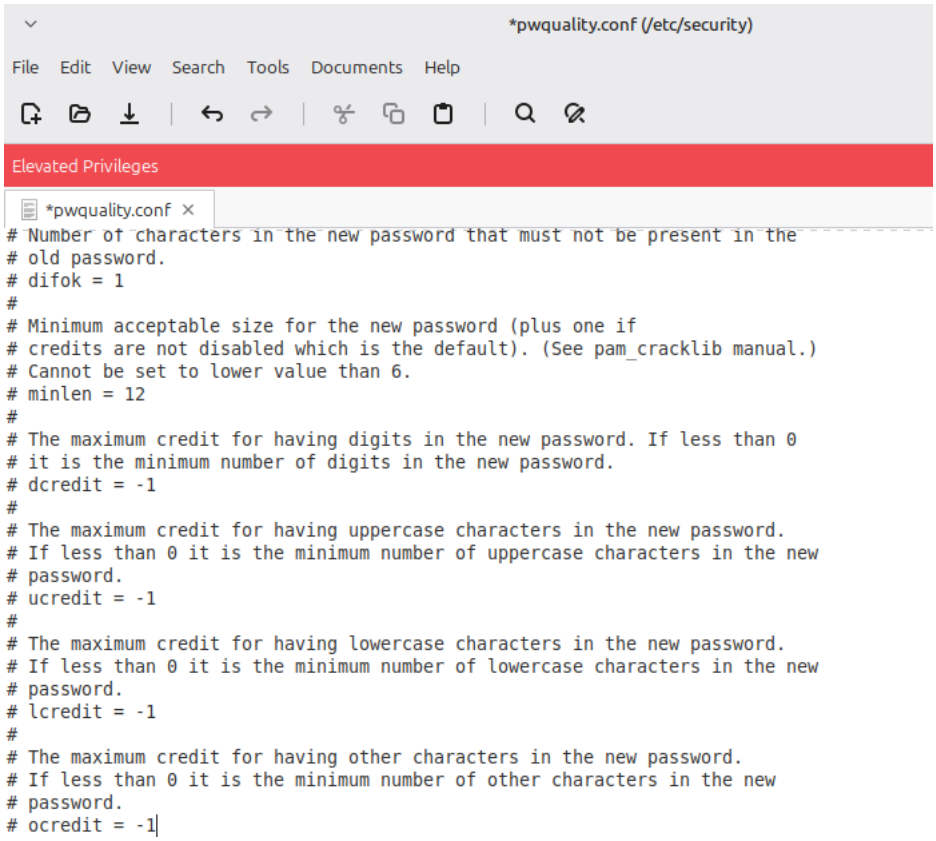


Рисунок 2 – Измененный файл `pwquality.conf`

```
# Требовать минимум 12 символов
# Требовать хотя бы одну цифру
# Требовать хотя бы одну заглавную букву
# Требовать хотя бы одну строчную букву
# Требовать хотя бы один специальный символ
```

В Linux Mint AppArmor уже установлен и активен. Наша задача – проверить его статус и понять, как он работает.

```
# Проверяем статус сервиса AppArmor
sudo systemctl status apparmor

# Проверяем, какие профили сейчас активны
sudo aa-status
```

Мы увидим список профилей. Часть из них в режиме `enforce` (принудительное исполнение правил), часть – в `complain` (только логирование нарушений). Для АС класса 1В все критически важные сервисы должны быть в режиме `enforce`.

```
root@mint:~# sudo aa-status
apparmor module is loaded.
1 profiles are loaded.
1 profiles are in enforce mode.
   rsyslogd
0 profiles are in complain mode.
0 profiles are in prompt mode.
0 profiles are in kill mode.
0 profiles are in unconfined mode.
1 processes have profiles defined.
1 processes are in enforce mode.
   /usr/sbin/rsyslogd (1234) rsyslogd
0 processes are in complain mode.
0 processes are in prompt mode.
0 processes are in kill mode.
0 processes are unconfined but have a profile defined.
0 processes are in mixed mode.
root@mint:~#
```

Рисунок 3 – Скриншот вывода команды `sudo aa-status`

1.4.3 Настройка подсистемы регистрации и учета

```
# Устанавливаем демон аудита и плагины
sudo apt install auditd audispd-plugins -y
# Создаем и открываем файл для правил
sudo nano /etc/audit/rules.d/10-security.rules
```

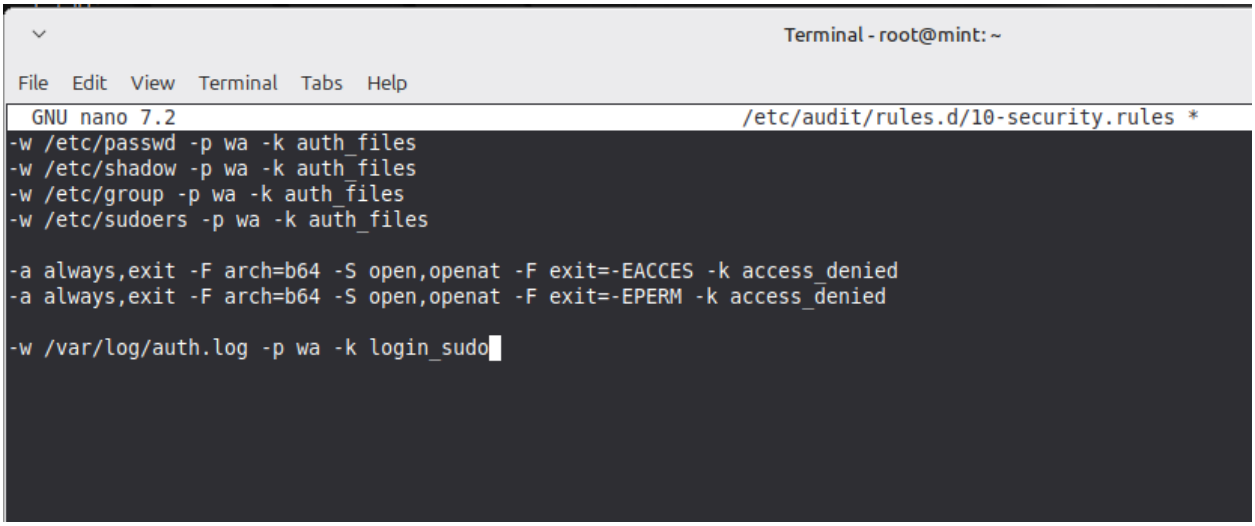


Рисунок 4 – Измененный файл `10-security.rules`

```
## Отслеживание любых изменений в файлах аутентификации и прав

## Отслеживание неудачных попыток доступа к файлам

## Отслеживание входа в систему и использования sudo

# Перезапускаем сервис
sudo systemctl restart auditd
```

Проверка логов:

```
# Ищем события, помеченные ключом "auth_files"
sudo ausearch -k auth_files
```

1.4.4 Настройка подсистемы обеспечения целостности

AIDE (Advanced Intrusion Detection Environment) создает "снимок" файловой системы и позволяет отслеживать любые несанкционированные изменения.

```
# Устанавливаем AIDE
sudo apt install aide -y
# Запускаем инициализацию
sudo aideinit
```

После завершения новая база данных будет сохранена в `/var/lib/aide/aide.db.new`. Мы должны переименовать ее, чтобы сделать "эталонной".

```
# Копируем новую базу в качестве эталона
sudo cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
# Запускаем проверку целостности
sudo aide –check
```

Если изменений не было, вывод будет содержать сообщение об этом. Если файлы менялись, вы увидите подробный отчет.

1.4.5 Настройка дополнительных мер защиты

Для обеспечения конфиденциальности коммерческой тайны (КТ) при физическом доступе к носителю (например, в случае кражи диска) необходимо применять полное шифрование диска. В Linux Mint эта мера реализуется с помощью стандартной технологии **LUKS (Linux Unified Key Setup)**.

1.4.5.1 Реализация

Данная мера защиты настраивается на этапе установки операционной системы. Для этого необходимо:

1. В меню инсталлятора "Тип установки" выбрать опцию **"Стереть диск и установить Linux Mint"**.
2. Активировать чекбокс **"Зашифровать установку Linux Mint для безопасности"**.
3. На следующем шаге задать и подтвердить **парольную фразу**, которая будет использоваться для расшифровки диска при каждой загрузке системы.

1.4.5.2 Проверка

Проверить, зашифрован ли диск, можно с помощью команды `lsblk`. В выводе для зашифрованной системы должен присутствовать логический том с типом `crypt`.

2 WHONIX

2.1 Предопределить дистрибутив

В Whonix, как системе, ориентированной на анонимность, защищаемым эндпоинтом скорее всего является Whonix Gateway, через который проходят все сетевые запросы, обеспечивая анонимность через сеть Tor (The Onion Router). Однако, если речь идет о защите государственной тайны, то таким эндпоинтом может быть сервер или система, которая обрабатывает эти данные, и которая должна быть дополнительно защищена.

2.2 Определить в какой системе расположен защищаемый эндпоинт

Пример возможных защищаемых эндпоинтов:

1. Whonix Gateway:
   - Это может быть защищаемый эндпоинт, если вся информация, включая данные о государственной тайне, маршрутизируется через Tor, а безопасность обеспечивается на уровне сетевых соединений.
   - Для повышения безопасности вы можете настроить дополнительные слои защиты, например, шифрование всего трафика, усиление контроля за подключениями через фаерволл и мониторинг соединений.
2. Рабочая станция (Whonix Workstation):
   - Это вторая виртуальная машина, используемая для выполнения задач с защищаемыми данными. Если данные обрабатываются на уровне операционной системы, на уровне пользователя, то такой рабочий компьютер можно считать защищаемым эндпоинтом.

2.3 Предопределить требования к защите с помощью нормативной базы

Для обеспечения надлежащей защиты в системе Whonix в контексте работы с конфиденциальной или государственной тайной необходимо учитывать несколько ключевых аспектов безопасности и соответствовать требованиям нормативных документов, регулирующих защиту данных и их обработку.

Нормативная база для защиты в Whonix

Защита данных и обеспечение безопасности в Whonix или в любой другой системе, работающей с конфиденциальной информацией, требует соответствия определенным стандартам и нормативам. Ниже перечислены основные нормативные документы и стандарты, которые могут быть полезны при защите системы, такой как Whonix:

1.2.1 Государственные стандарты

1. Федеральный закон от 21 июля 1993 года № 5485-1 "О государственной тайне"

Этот закон является основным актом, регулирующим классификацию информации как государственной тайны, порядок ее защиты и ответственности за утечку сведений.

2. ГОСТ Р 50739-95 "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования"

Стандарт определяет общие технические требования к средствам вычислительной техники, обеспечивающим защиту от несанкционированного доступа к информации. Rosgosts

3. ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения"

Этот стандарт устанавливает основные термины и определения, применяемые при проведении работ по стандартизации в области защиты информации. Stroyinf Files

4. Приказ ФСБ России от 25 ноября 2002 года № 255 "Об утверждении инструкций по защите государственной тайны"

Приказ ФСБ России, утверждающий инструкции по защите государственной тайны, включая организационные и технические требования.

5. Приказ Министерства обороны России № 400 "Об утверждении инструкции по работе с секретными документами"

Этот приказ распространяется на государственные органы и органы обороны, которые работают с секретной информацией, включая процедуру доступа, хранения и уничтожения секретных материалов.

2.4 Выполнить настройку Unix системы в соответствии с требованиями регуляторов

1.3.1 Включаем AppArmor

sudo apt install apparmor apparmor-utils

sudo systemctl enable apparmor

sudo systemctl start apparmor

```
[workstation user ~]% sudo apt install apparmor apparmor-utils

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apparmor is already the newest version (3.0.8-3).
apparmor set to manually installed.
apparmor-utils is already the newest version (3.0.8-3).
apparmor-utils set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
[workstation user ~]% sudo systemctl enable apparmor
Synchronizing state of apparmor.service with SysV service script with /lib/syste
md/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apparmor
```

1.3.2 Используем шифрование данных

A) Шифрование жесткого диска с использованием LUKS

Сначала нужно создать защищаемый диск

dd if=/dev/zero of=/home/user/virtual_disk.img bs=1M count=1024

```
[workstation user ~]% dd if=/dev/zero of=/home/user/virtual_disk.img bs=1M count
=1024

1024+0 records in
1024+0 records out
1073741824 bytes (1.1 GB, 1.0 GiB) copied, 0.79328 s, 1.4 GB/s
```

Примение шифрования LUKS к файлу-диску

sudo cryptsetup luksFormat /home/user/virtual_disk.img

```
[workstation user ~]% sudo cryptsetup luksFormat /home/user/virtual_disk.img


WARNING!
========
This will overwrite data on /home/user/virtual_disk.img irrevocably.

Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for /home/user/virtual_disk.img:
Verify passphrase:
```

В качестве тестовой кодовой фразы было использовано имя Artem

После того как диск будет зашифрован, его нужно "открыть" с использованием cryptsetup для монтирования.

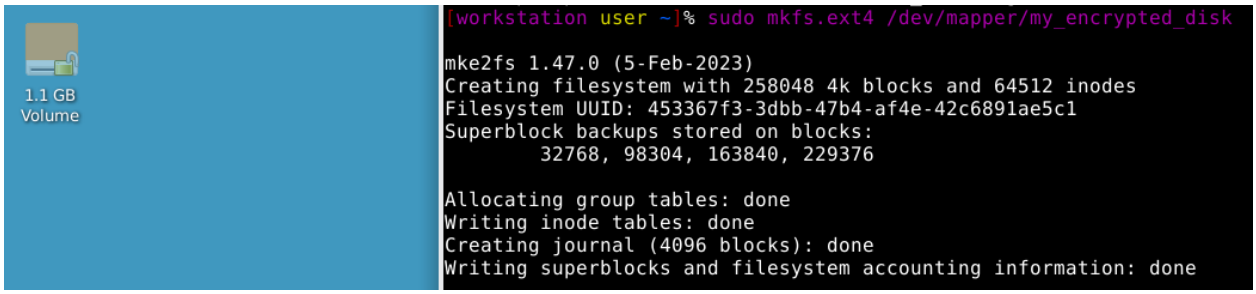
sudo cryptsetup luksOpen /home/user/virtual_disk.img my_encrypted_disk

```
[workstation user ~]% sudo cryptsetup luksOpen /home/user/virtual_disk.img my_en
crypted_disk

Enter passphrase for /home/user/virtual_disk.img:
```

После того как диск будет открыт, нужно создать файловую систему, чтобы можно было его использовать

sudo mkfs.ext4 /dev/mapper/my_encrypted_disk



Создаем точку монтирования sudo mkdir /mnt/encrypted

Монтируем диск sudo mount /dev/mapper/my_encrypted_disk /mnt/encrypted

```
[workstation user ~]% sudo mkdir /mnt/encrypted

[workstation user ~]% sudo mount /dev/mapper/my_encrypted_disk /mnt/encrypted
```

Теперь, когда мы создали зашифрованный диск, мы можем использовать его как обычный диск, но с дополнительным уровнем безопасности. Все данные на этом диске будут зашифрованы и могут быть доступны только после ввода пароля.

1.3.3 Аудит и мониторинг

Для выполнения требований аудита, используем auditd для отслеживания действий в системе.

Устанавливем sudo apt install auditd

Включаем отслеживание всех изменений в файле sudoers, таким образом мы будем знать о любой попытке доступа к всем возможным файлам

-w /etc/sudoers -p wa -k sudoers_changes

Для применения настроек перезапускаем

sudo systemctl restart auditd

1.3.4 Сетевые настройки безопасности

Используем Firewall

sudo ufw enable

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow ssh

3 ГОСТ ОТВЕЧАЕТ НА СЛЕДУЮЩИЕ ВОПРОСЫ

• Какие угрозы безопасности появляются, когда мы используем виртуальные машины (ВМ) вместо физических серверов?

• Как правильно настроить и управлять виртуальной инфраструктурой, чтобы она была защищена?

• Какие требования предъявляются к средствам защиты информации (СЗИ) в такой среде?

Ответы:

1. Виртуализация добавляет новый уровень атаки — **гипервизор**. Основные угрозы:

- **Компрометация гипервизора:** Захват одного гипервизора дает злоумышленнику контроль над **всеми** ВМ на нем.
- **Атаки между ВМ:** Скомпрометированная ВМ может атаковать соседние ВМ на том же физическом сервере.
- **"Побег" из ВМ (VM Escape):** Вредоносный код "вырывается" из ВМ и получает доступ к гипервизору.
- **Атаки на средства управления:** Взлом консоли управления (vCenter, zVirt) равносилен захвату всей инфраструктуры.
- **Невидимый трафик:** Сетевые взаимодействия между ВМ на одном хосте (east-west) могут обходить физические файрволы, оставаясь незамеченными.

2. Защита должна быть комплексной и охватывать все новые компоненты:

- **Усиление безопасности гипервизора:** Устанавливать только необходимые компоненты, своевременно обновлять, строго ограничивать доступ к управлению.
- **Сетевая сегментация:** Изолировать ВМ разных уровней важности друг от друга с помощью виртуальных сетей (VLAN) и межсетевых экранов.
- **Защита управления:** Применять многофакторную аутентификацию для администраторов, вести детальный аудит их действий.
- **Контроль жизненного цикла ВМ:** Внедрить строгие политики создания, обновления и удаления ВМ и их снимков (снапшотов), чтобы избежать появления "забытых" уязвимых машин.
- **Мониторинг и аудит:** Централизованно собирать и анализировать все события безопасности, происходящие в виртуальной среде.

3. Средства защиты информации (СЗИ) должны быть адаптированы к виртуализации:

- **Поддержка виртуализации ("Virtualization-Aware"):** СЗИ должны понимать, что работают в виртуальной среде, и быть оптимизированы для нее (например, безагентные антивирусы).
- **Контроль трафика "east-west":** Межсетевые экраны должны фильтровать трафик не только на периметре, но и **между ВМ** на одном хосте.
- **Интеграция с API платформы:** СЗИ должны взаимодействовать с системой управления виртуализацией, чтобы автоматически применять политики к новым и перемещаемым ВМ.
- **Защита самого гипервизора:** Необходимы специализированные решения для контроля целостности и конфигурации хостов виртуализации.

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы была настроена операционная система Linux Mint в соответствии с требованиями, предъявляемыми к автоматизированным системам класса 1В и системам, обрабатывающим коммерческую тайну. Были реализованы следующие ключевые меры защиты:

- Усилена политика аутентификации пользователей.
- Настроен мандатный контроль доступа с помощью AppArmor.
- Внедрена система детального аудита событий безопасности auditd.
- Развернута система контроля целостности системных файлов AIDE.
- Настроен межсетевой экран с политикой "запрещено по умолчанию".
- Обеспечено шифрование данных на диске с помощью LUKS.

Реализованный комплекс мер позволяет обеспечить необходимый уровень защищенности информации от несанкционированного доступа в соответствии с заданием.

Также мы организовали защиту уровня “Государственная тайна” на системе Whonix, использовали шифрование конкреного репозитория, организовали мониторинг и аудит системы, так же используем AppArmor как пример разграничения доступа. Преимущества изоляции с использованием Whonix и виртуализации:

1. Изоляция приложений: Использование Whonix-Gateway для маршрутизации всего интернет-трафика через Tor помогает гарантировать анонимность, а изоляция Whonix-Workstation предотвращает утечку информации.

2. Безопасность данных: Вы можете дополнительно зашифровать диски, использовать сильные пароли и защищенные каналы для передачи конфиденциальной информации.

3. Гибкость: Виртуальные машины позволяют вам запускать несколько изолированных рабочих сред на одном компьютере, что дает возможность работать с различными уровнями конфиденциальности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Лазутин А. И. Курс лекций по дисциплине «Программно-аппаратные средства защиты информации» / А. И. Лазутин, Армавир, 2023. – Текст: непосредственный.
2. Руководящий документ от 30 марта 1992 г. - ФСТЭК России – Текст : электронный. – 1992.
3. Федеральный закон от 29.07.2004 г. № 98-ФЗ • Президент России – Текст : электронный. – 2004.
4. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 - ФСТЭК России – Текст : электронный. – 2013.
5. ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения – Текст : электронный. – 2016.