

**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 ПРАКТИЧЕСКОЙ РАБОТЕ №2**

**«Механизмы защиты Unix систем»**

**Выполнили:**

Нгуен Тхе Вьет, студент группы N3347



(подпись)

Чу Ван Доан, студент группы N3347



(подпись)

Доан Тхи Хоай Тхыонг, студентка группы N3345



(подпись)

Чан Бао Линь, студентка группы N3346



**Проверил:**

Калабишка Михаил Михайлович, Преподаватель ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2024 г

## СОДЕРЖАНИЕ

Содержание	2
Список сокращений	3
Введение	4
1    Определение дистрибутива и информационной системы	5
1.1    Debian	5
1.2    Система АС 2Б	6
2    Требования к защите автоматизированной системы класса 2Б	7
3    Настройка Debian в соответствии с требованиями регуляторов	10
3.1    Настройка подсистемы управления доступом	10
3.2    Настройка подсистемы регистрации и учета	11
3.3    Настройка подсистемы обеспечения целостности	13
Заключение	19
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	20

## **СПИСОК СОКРАЩЕНИЙ**

ИС – Информационная система

АС – Автоматизированные системы

НСД – Несанкционированный доступ

СЗИ – Система защиты информации

СЗИ НСД – Система защиты информации от несанкционированного доступа

## **ВВЕДЕНИЕ**

Цель работы – ознакомление с базовыми модулями защиты Unix систем.

Для достижения цели работы, необходимо решать 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 ОПРЕДЕЛЕНИЕ ДИСТРИБУТИВА И ИНФОРМАЦИОННОЙ СИСТЕМЫ**

Выбранный вариант – 11

Дистрибутив – Debian

ИС – АС 2Б

Список сокращений:

ИС – Информационная система

АС – Автоматизированные системы

НСД – Несанкционированный доступ

СЗИ – Система защиты информации

СЗИ НСД – Система защиты информации от несанкционированного доступа

## **1.1 Debian**

Debian — это популярный и широко используемый дистрибутив Linux с открытым исходным кодом. Он служит основой для многих других дистрибутивов Linux, таких как Ubuntu и Linux Mint. Основные особенности Debian включают:

- Система управления пакетами: Debian использует Advanced Package Tool (APT) и пакеты формата .deb для установки и управления программами. Это упрощает установку, обновление и удаление программного обеспечения с помощью простых команд.
- Свободное и открытое программное обеспечение: Debian ориентирован на использование только свободного и открытого программного обеспечения, что делает его идеальным выбором для пользователей, которые ценят свободу программного обеспечения и прозрачность кода.
- Стабильность и надёжность: Debian известен своей стабильностью. У него есть три основные ветки: stable (стабильная), testing (тестовая) и unstable (нестабильная). Ветка stable тщательно протестирована и считается готовой для использования на производственных системах, а ветки testing и unstable содержат более новые версии ПО, но могут быть менее стабильными.
- Разработка, управляемая сообществом: Debian разрабатывается и поддерживается глобальным сообществом добровольцев. Решения и улучшения принимаются через

демократический процесс в рамках проекта Debian.

- Универсальность: Debian может использоваться как настольная операционная система, серверная система, а также встраиваться в устройства. Он поддерживает широкий спектр аппаратных архитектур, включая x86, ARM и другие.

## **1.2 Система АС 2Б**

Автоматизированная система (АС) — это система, которая состоит из персонала и комплекса средств автоматизации, предназначенных для поддержки и оптимизации их деятельности. Она реализует информационные технологии для выполнения определённых, заранее установленных функций.

Автоматизированная система класса 2Б характеризуется равными правами доступа для всех пользователей ко всей информации, хранящейся или обрабатываемой в системе, независимо от уровня конфиденциальности данных. Это означает, что каждый пользователь имеет одинаковые права на просмотр и изменение любых данных, включая чувствительную информацию, такую как служебная тайна или персональные данные.

## **2 ТРЕБОВАНИЯ К ЗАЩИТЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КЛАССА 2Б**

Из руководящего документа ФСТЭК от 30 марта 1992 года:

Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

1.4. Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД

1.5. Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

1.6. Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

1.7. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС - коллективный или индивидуальный.

1.8. Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

1.9. Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.



# Автоматизированные системы

Третья группа		Вторая группа		Первая группа				
Однопользовательская		Многопользовательская с равными полномочиями		Многопользовательская с разными полномочиями				
Уровень конфиденциальности информации								
НС	ОВ, СС, С	НС	ОВ, СС, С	НС	НС	С	СС	ОВ
Классы защищенности								
3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А

Рисунок 1 – Классы защищенности.

## 2. Требования по защите информации от НСД для АС

2.1. Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

2.2. В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

## 2.3. Требования к классу защищенности 2Б:

Подсистема управления доступом: должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и 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);
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

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 во время обработки и (или) хранения защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программы, 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.

### 3 НАСТРОЙКА DEBIAN В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ РЕГУЛЯТОРОВ

#### 3.1 Настройка подсистемы управления доступом

Сначала мы создаем новый пользователь (рис. 2)

```
root@vbox:~# useradd user1
root@vbox:~# passwd user1
New password:
Retype new password:
passwd: password updated successfully
```

Рисунок 2 – Создание новой пользователя

Затем осуществляем идентификацию и аутентификацию субъектов доступа при входе в систему с использованием идентификационного кода (кода) и условного фиксированного пароля, состоящего не менее чем из 8 символов и содержащего не менее чем 3 класса символов (рис. 3).

```
GNU nano 7.2 /etc/pam.d/common-password

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11. Without this option, the default is Unix crypt. Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility. The "obscure" option replaces the old
#`OBSOLETE_CHECKS_ENAB' option in login.defs. See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      requisite          pam_pwquality.so retry=3          minlen=12          difok=3
password      [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt
# here's the fallback if no module succeeds
password      requisite          pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required           pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional          pam_gnome_keyring.so
# end of pam-auth-update config
```

```
GNU nano 7.2 /etc/security/pwquality.conf *
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 12
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
minclass = 3
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Рисунок 3 – Правил установки пароля

Потом проверяем правила установки пароля. Мы видим, что если пароль состоит из менее чем 12 символов или включает в себя менее чем 3 класса символов, то пароль считается недействительным и мы не можем изменить пароль (рис. 4).

```
root@vbox:~# passwd user1
New password:
BAD PASSWORD: The password is shorter than 12 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains less than 3 character classes
Retype new password:
Sorry, passwords do not match.
New password:
Retype new password:
passwd: password updated successfully
```

Рисунок 4 – Попытка ввести новый пароль

### 3.2 Настройка подсистемы регистрации и учета

Все файлы журналов, можно отнести к одной из следующих категорий:

- приложения;
- события;
- службы;
- системный.

Большинство лог файлов содержится в директории /var/log:

- /var/log/syslog или /var/log/messages содержит глобальный системный журнал, в котором пишутся сообщения с момента запуска системы, от ядра Linux, различных служб, обнаруженных устройствах, сетевых интерфейсов и много другого.
- /var/log/auth.log или /var/log/secure — информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации.
- /var/log/dmesg — драйвера устройств. Одноименной командой можно просмотреть вывод содержимого файла. Размер журнала ограничен, когда файл достигнет своего предела, старые сообщения будут перезаписаны более новыми. Задав ключ --level= можно отфильтровать вывод по критерию значимости.

```
root@vbox:~# ls /var/log
alternatives.log  faillog          private
apt               fontconfig.log  README
boot.log          gdm3             speech-dispatcher
btmtp             installer        vboxpostinstall.log
cups              journal          wtmp
dpkg.log          lastlog
```

Рисунок 5 – Список записи о различных системных и прикладных событиях

```

debian@vbox:~$ last
debian    tty2          tty2          Mon Nov  4 20:29    still logged in
reboot    system boot    6.1.0-26-amd64 Mon Nov  4 20:26    still running
debian    tty2          tty2          Fri Nov  1 19:40    - crash (3+00:46)
reboot    system boot    6.1.0-26-amd64 Fri Nov  1 19:40    still running
debian    tty2          tty2          Fri Nov  1 19:38    - crash (00:01)
reboot    system boot    6.1.0-26-amd64 Fri Nov  1 19:38    still running
debian    tty2          tty2          Fri Nov  1 19:22    - crash (00:15)
reboot    system boot    6.1.0-26-amd64 Fri Nov  1 19:21    still running

```

Рисунок 6 – Журнал входа и выхода пользователей

```

debian@vbox:~$ su
Password:
su: Authentication failure
debian@vbox:~$ su
Password:
root@vbox:/home/debian# lastb
root      pts/1          Tue Nov  5 00:00 - 00:00 (00:00)

btmpt begins Tue Nov  5 00:00:14 2024

```

Рисунок 7 – Журнал неудачных попыток входа в систему

Команда `dmesg` используется для отображения сообщений ядра операционной системы в Unix-подобных системах, включая Debian. Для поиска информации, связанной с конкретным устройством, таким как жесткий диск, идентифицированный как "sda", мы можем использовать команду `dmesg` с командой `grep`.

```

root@vbox:/home/debian# dmesg | grep sda
[ 1.370544] sd 2:0:0:0: [sda] 41943040 512-byte logical blocks: (21.5 GB/20.0 GiB)
[ 1.370549] sd 2:0:0:0: [sda] Write Protect is off
[ 1.370550] sd 2:0:0:0: [sda] Mode Sense: 00 3a 00 00
[ 1.370554] sd 2:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[ 1.370559] sd 2:0:0:0: [sda] Preferred minimum I/O size 512 bytes
[ 1.377907] sda: sda1 sda2 < sda5 >
[ 1.378023] sd 2:0:0:0: [sda] Attached SCSI disk
[ 1.959143] EXT4-fs (sda1): mounted filesystem with ordered data mode. Quota mode: none.
[ 2.396170] EXT4-fs (sda1): re-mounted. Quota mode: none.
[ 3.175131] Adding 998396k swap on /dev/sda5. Priority:-2 extents:1 across:998396k FS

```

Рисунок 8 – Журнал носителей информации

Эта команда отобразит сообщения ядра, связанные с устройством "sda" (обычно это жесткий диск) в нашей системе. Мы увидим информацию о инициализации устройства, разделах и связанных событиях или ошибках в выводе.



### 3.3 Настройка подсистемы обеспечения целостности

В качестве СЗИ мы выбрали бесплатный антивирус ClamAV. Его конфигурационные файлы находятся по пути `/etc/clamav/clamd.conf` и `/etc/clamav/freshclam.conf`. Используем хеш-функцию `sha256` для проверки целостности конфигов. Значения хеш-функции показаны на рисунке 9.

```
debian@vbox:~$ ls -la /etc/clamav/
total 36
drwxr-xr-x  5 root  root  4096 Nov  5 00:18 .
drwxr-xr-x 121 root  root 12288 Nov  5 00:18 ..
-rw-r--r--  1 root  root  1994 Nov  5 00:18 clamd.conf
-r--r--r--  1 clamav adm   682 Nov  5 00:18 freshclam.conf
drwxr-xr-x  2 root  root  4096 Feb  8 2024 onerrorexecute.d
drwxr-xr-x  2 root  root  4096 Feb  8 2024 onupdateexecute.d
drwxr-xr-x  2 root  root  4096 Feb  8 2024 virusevent.d
```

Рисунок 9 – Проверка целостности файла до его изменения

```
GNU nano 7.2 hash_gen.sh *
#!/bin/bash

#Define the folder path and output file name
folder="/etc/clamav"
output_file="hashes"

#Generate hashsum for each file in the folder
find "$folder" -type f | while IFS= read -r file; do
    hashsum=$(sha256sum "$file" | awk '{print $1}')
    echo "$hashsum $file"
done > "$output_file"
```

Рисунок 10 – Баш скрипт для генерации Хеш-суммы



```

GNU nano 7.2                                check_gen.sh *
#!/bin/bash

#Define the folder path and hash file name
folder="/etc/clamav"
hash_file="hashes"

#Verify integrity of each file in the folder
while read -r line; do
    hashsum=$(echo "$line" | awk '{print $1}')
    file=$(echo "$line" | awk '{print $2}')
    # check if the file exists
    if [ ! -f "$file" ]; then
        echo "File $file does not exists."
        continue
    fi
    #Calculate the hashsum of the file
    calculated_hashsum=$(sha256sum "$file" | awk '{print $1}')

    #Compare the calculated hashsum with the expected hashsum
    if [ "$hashsum" = "$calculated_hashsum" ]; then
        echo "File $file is intact."
    else
        echo "File $file has been modified!"
    fi
done < "$hash_file"

```

Рисунок 11 – Bash скрипт для сравнения рассчитанной с ожидаемой хеш-суммой

```

root@vbox:/home/debian# sh ./hash_gen.sh
root@vbox:/home/debian# cat hashes
e79b36747f6f5d350b33d8ccbad29f4434f7ee8164080aefe5a1360924575126 /etc/clamav/clamd.conf
e3554a15c0fe412004cc401718e03e6bc65cabf3b0fe2bed744829c76110f0bb /etc/clamav/freshclam.conf
root@vbox:/home/debian# sh ./check_gen.sh
File /etc/clamav/clamd.conf is intact.
File /etc/clamav/freshclam.conf is intact.
root@vbox:/home/debian# nano /etc/clamav/clamd.conf
root@vbox:/home/debian# sh ./check_gen.sh
File /etc/clamav/clamd.conf has been modified!
File /etc/clamav/freshclam.conf is intact.

```

Рисунок 12 – Проверка работы скрипта

```
GNU nano 7.2 /tmp/crontab.W2IvZ8/crontab *
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow command
@reboot /home/debian/check_hash.sh
```

Рисунок 13 – Внесение скрипта в crontab

/home/thanh/check\_hash.sh тут идет запуск bash скрипта. Теперь после сохранения файла и перезагрузки устройства запустится bash скрипт.

Затем мы используем приложение “Backintime” для создания резервного копирования. Мы можем сохранить резервное копирование в Local или с помощью SSH для удаленного подключения. Кроме того, мы можем запланировать резервное копирование в разделе “Schedule” (рис. 14).

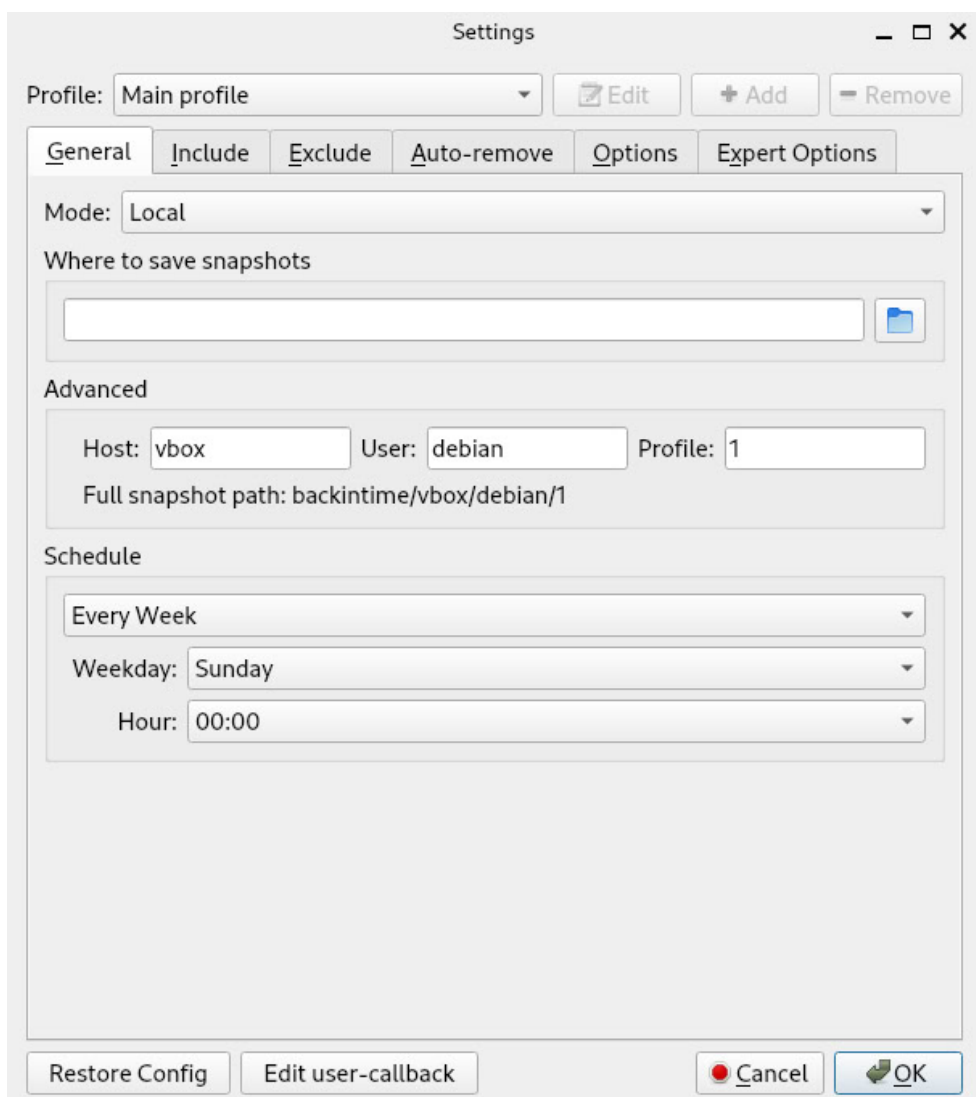


Рисунок 14 – приложение “Backintime”

Include позволяет указать файлы и папки, exclude позволяет таким же образом исключать папки.

После запуска приложения его настройка достаточно проста. На главном экране перечислены все резервные копии (Backintime называет их "снимками").

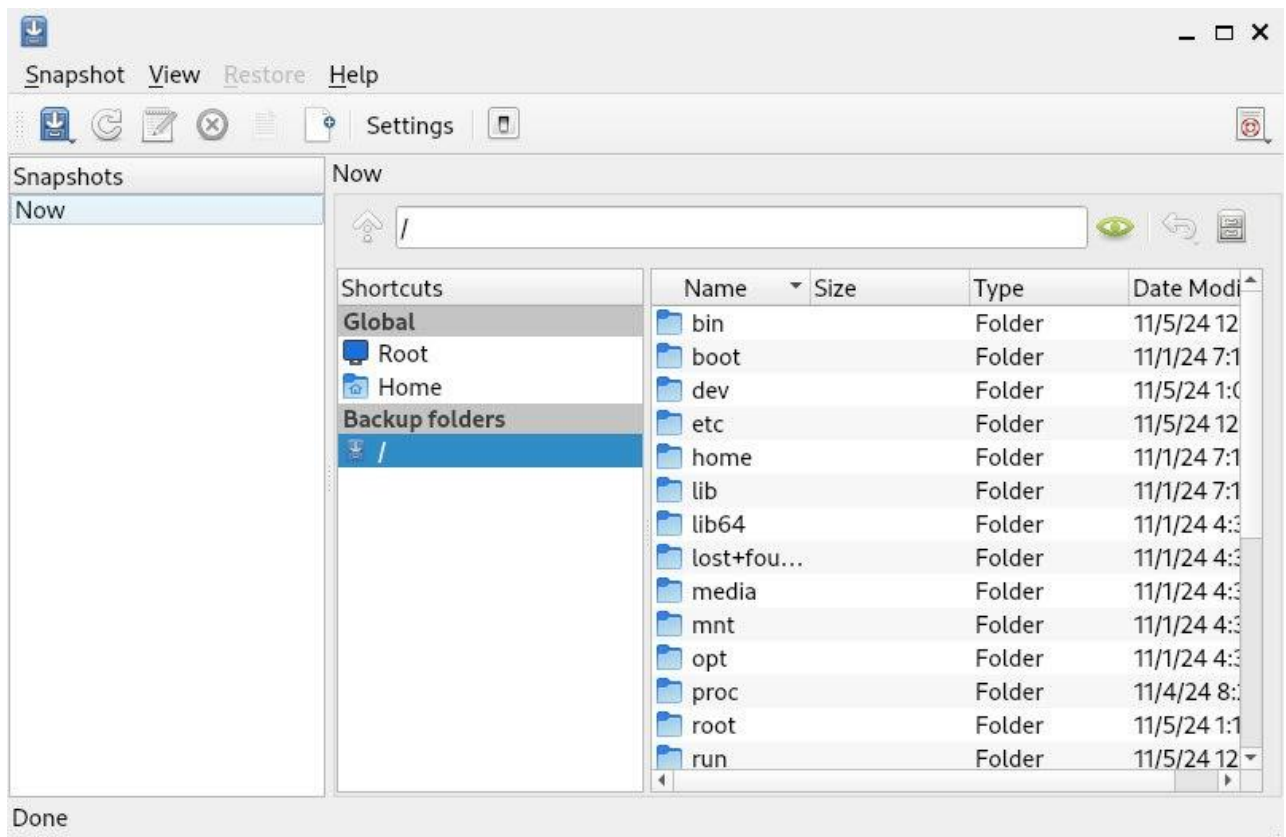


Рисунок 15 – Интерфейс программы

Здесь можно работать со всеми бэкапами. Восстанавливать, удалять, сравнивать и т.д. Выбрав нужный нажмите на уже знакомую кнопку «Восстановить». После завершения работы все данные будут восстановлены.


Для периодического тестирования функций СЗИ с помощью тест-программы из доступного и подходящего под Debian 12 мы выбрали Vulners agent. Агент собирает информацию об ОС, ее версии и любых установленных пакетах. Затем эта информация отправляется в Vulners API, чтобы выяснить, какое программное обеспечение уязвимо.

```
root@vbox:/etc/vulners# cat vulners_agent.conf
[DEFAULT]
api_key = 3U8FGK53SDTSLJ67XKG579BJZ4PVETEBCSV07D1FTQSP2YPORSD6A08KCSKQU
```


Рисунок 16 – Добавление api-key для использования vulners agent

```
root@vbox:/etc/vulnervulners-agent --app Scanner
2024-11-05 18:24:08,250 - Ticker - INFO - There is no data file. Informational.
2024-11-05 18:24:08,250 - Ticker - INFO - Application Ticker: Waiting for queue to perform action - estimated waiting time is 129 seconds
2024-11-05 18:26:34,267 - Ticker - INFO - There is no data file. Informational.
2024-11-05 18:26:34,890 - Ticker - INFO - There is no data file. Informational.
2024-11-05 18:26:35,114 - Scanner - INFO - Application Scanner: Waiting for queue to perform action - estimated waiting time is 123 seconds
2024-11-05 18:28:49,655 - Scanner - INFO - Scan complete. Check your result at https://vulners.com/scan
2024-11-05 18:28:49,665 - Scanner - INFO - Application Scanner: Waiting for queue to perform action - estimated waiting time is 282 seconds
2024-11-05 18:33:53,457 - Scanner - INFO - Scan complete. Check your result at https://vulners.com/scan
root@vbox:/etc/vulners#
```


Рисунок 17 – Запуск сканера



New agent scanner  
Scan using windows or linux agent



New API scanner  
Create your own security tool or plugin



New Manual scan  
Paste list of packages to analyze

Agent IP  
10.0.2.15

Agent FQDN

OS Name

Clear X



OS Version

OS Family

Severity

Vulnerability ID

Tags

OS	OS Version	CVSS Score	IP	FQDN	Scan Date	
	12	10	10.0.2.15	vbox.NetisRoute...	2024-11-05 15:28:48	
	12	10	10.0.2.15	vbox.NetisRoute...	2024-11-05 15:33:53	

count 30

ID	Severity	Family	Title	Agent IP	Agent FQDN
DEBIANCVE...	critical	debiancve	CVE-2023-6816	10.0.2.15	vbox.NetisF
DEBIANCVE...	critical	debiancve	CVE-2023-40359	10.0.2.15	vbox.NetisF
DEBIANCVE...	critical	debiancve	CVE-2016-1585	10.0.2.15	vbox.NetisF
DEBIANCVE...	critical	debiancve	CVE-2005-2541	10.0.2.15	vbox.NetisF
DEBIANCVE...	high	debiancve	CVE-2024-9632	10.0.2.15	vbox.NetisF
DEBIANCVE...	high	debiancve	CVE-2024-34459	10.0.2.15	vbox.NetisF
DEBIANCVE...	high	debiancve	CVE-2024-31083	10.0.2.15	vbox.NetisF
DEBIANCVE...	high	debiancve	CVE-2024-31081	10.0.2.15	vbox.NetisF
DEBIANCVE...	high	debiancve	CVE-2024-31080	10.0.2.15	vbox.NetisF
DEBIANCVE...	high	debiancve	CVE-2024-25062	10.0.2.15	vbox.NetisF

OS Name debian

OS Version 12


Installed Package xwayland 2:22.1.9-1 amd64

Should be installed xorg-server 2:21.1.7-3+deb12u5 xwayland 2:22.1.9-1

CVE-2023-6816

How to Fix

sudo apt-get --assume-yes install --only-upgrade xwayland

 CVE-2023-6816  
2024-01-18 08:15

cvss 9.8  
cvss3 9.8  
7.5

ID DEBIANCVE:CVE-2023-6816  
Type debiancve  
Reporter Debian Security Bug Tracker  
Modified 2024-01-18 08:15  
CVSS v3

Agent IP	Agent FQDN	OS Name	OS Version	Clear X		
OS Family	Severity	Vulnerability ID	Tags			
ID	Severity	Count	Family	Title	Score	
DEBIANCVE:CVE-2023-40359	critical	1	debiancve	CVE-2023-40359	9.8	
DEBIANCVE:CVE-2023-6816	critical	1	debiancve	CVE-2023-6816	9.8	
DEBIANCVE:CVE-2005-2541	critical	1	debiancve	CVE-2005-2541	10	
DEBIANCVE:CVE-2016-1585	critical	1	debiancve	CVE-2016-1585	9.8	
DEBIANCVE:CVE-2024-0229	high	1	debiancve	CVE-2024-0229	7.8	
DEBIANCVE:CVE-2023-30630	high	1	debiancve	CVE-2023-30630	7.1	
DEBIANCVE:CVE-2022-4055	high	1	debiancve	CVE-2022-4055	7.4	
DEBIANCVE:CVE-2024-25062	high	1	debiancve	CVE-2024-25062	7.5	
DEBIANCVE:CVE-2023-51596	high	1	debiancve	CVE-2023-51596	7.1	

Agent IP

Agent FQDN

OS Name

OS Version




OS Family

Clear X

Severity

Vulnerability ID

Tags

OS	Version	Score	IP	FQDN	Tags	Total Vulns	Vulnerabilities	
	12	587	10.0.2.15	vbox.NetisRoute... 		99	<div><div>20</div><div>42</div><div>33</div><div>4</div></div>	

Rows per page: 30

< 1-1 of 1 >

Рисунок 18 – Результаты сканирования

СЗИ ClamAV не допустил проникновения вирусов и других вредоносных программ.

## **ЗАКЛЮЧЕНИЕ**

В результате выполнения лабораторной работы была выполнена поставленная задача. Для настройки системы Debian были изучены требования руководящего документа ФСТЭК от 30 марта 1992 года, подобрана и реализована система СЗИ.



## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Классификация средств защиты информации от ФСТЭК и ФСБ России - URL: [https://www.anti-malware.ru/analytics/Market\\_Analysis/infosecurity-systems-classification-fsb-fstek](https://www.anti-malware.ru/analytics/Market_Analysis/infosecurity-systems-classification-fsb-fstek).
2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных системы требования по защите информации - URL: <https://docs.cntd.ru/document/901817219> .