ЛЕКЦИЯ 12. ОЧИСТКА ОТ НЕНУЖНЫХ ФАЙЛОВ И ВИРУСОВ LINUX

Linux Mint стабильная система, но в ней иногда накапливается ненужный мусор, который остается после удаления программ, ненужных зависимостей и т.д.

Удалить мусор можно при помощи Терминала, например, так:

sudo apt-get autoclean

- рекомендуется делать эту команду периодически, очищая систему от .deb пакетов, которые более не нужны,

sudo apt-get autoremove

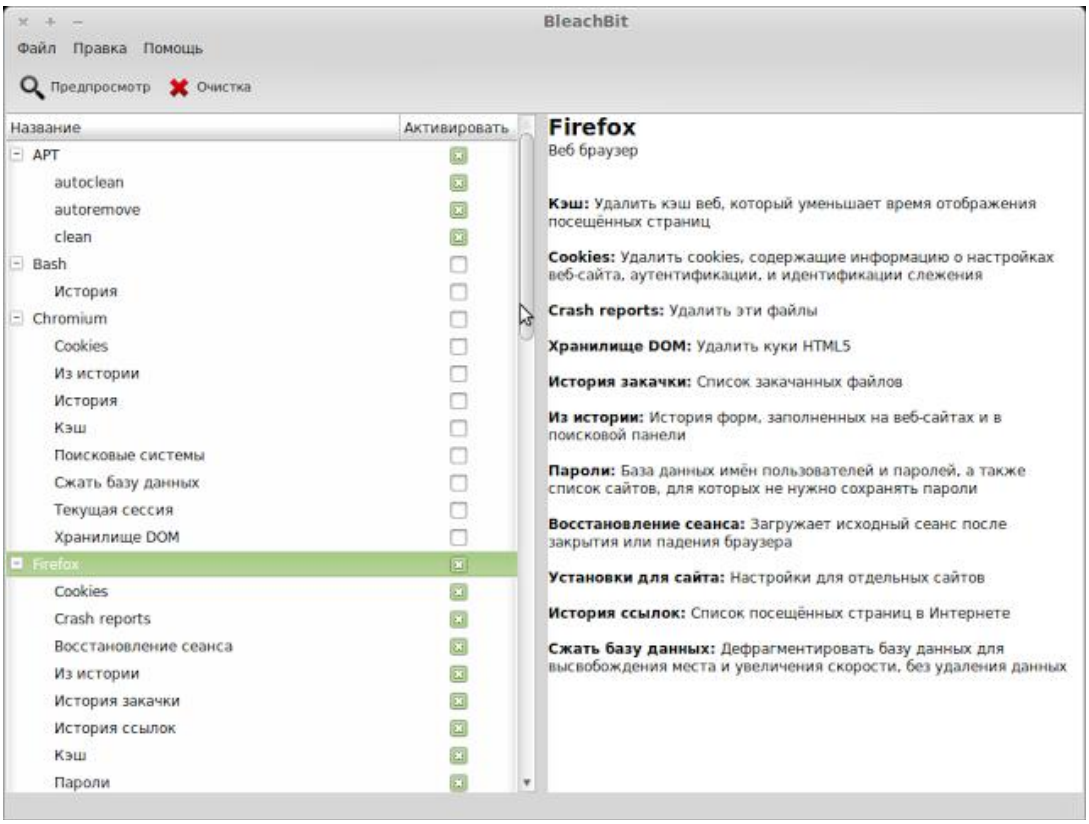
- данная команда удаляет неудалённые зависимости от уже удалённых пакетов,

sudo apt-get clean

- очистка каталога /var/cache/apt/archives/ .

12.1. BLEACHBIT - УТИЛИТА ДЛЯ ОЧИСТКИ СИСТЕМНОГО МУСОРА

BleachBit программа-чистильщик, которая предназначена для быстрой и легкой очистки операционной системы от накопившихся, мусорных файлов. Данная утилита разработана на основе кросс-платформенности и поэтому может быть установлена, как на *Windows* машине, так и в *Linux* системах. Со временем в системе скапливается огромное количество всевозможных временных и не нужных файлов, которые только занимают лишнее место и тормозят систему.



Особенно это актуально, если вам приходится много раз устанавливать и удалять разные приложения, в целях тестирования той или иной программы. После частых и продолжительных таких действий, в системе появляются гигабайты ненужного мусора.

BleachBit находит такие файлы и удаляет их. Надо отметить, что программа имеет очень высокую скорость работы. В официальном репозитории дистрибутива Mint, эта утилита несколько отстает по версии от последних официальных релизов, но честно говоря, это не очень актуально. Устанавливается программа обычным способом через "Менеджер программ" или консоль.

sudo apt-get install bleachbit

Если же, вы все-таки хотите иметь самую последнюю версию программы, то нужный пакет можно скачать с официального сайта программы, а заодно и установить дополнительный пакет *Bonus-pack,* который скачивается от туда же. После установки программы в меню:

Приложения→Системные утилиты→*BleachBit*

Там будет присутствовать два ярлыка программы. Один обычный, а второй с наименованием (*as root*). Для очистки директории (*/home*) можно пользоваться обычным запуском, а если необходимо очистить всю систему с соответствующими в программе настройками, то нужно запускать ярлык с атрибутами (*as root*). И напоследок помните, что *BleachBit* - это программа не ремонтирующая вашу систему или компьютер, а всего лишь, инструмент очистки, позволяющий облегчить вашу "операционку".

Характеристики *BleachBit:*

- хорошая русификация;
- наглядные разъяснения;
- удаление неактуальных интерфейсных языков;
- возможность очистки оперативной и виртуальной памяти;
- удаление самых разнообразных временных файлов;
- сжатие баз данных;
- вычищает ненужный мусор из, просто огромного списка используемых программ;
- чистит историю и кэш;
- чистит файлы *Windows* (*Thumbs.db*).

12.2. УСТАНАВЛИВАЕМ АНТИВИРУС BITDEFENDER

Антивирусы пользователям Mint не нужны. Вирусы в Mint могут появляться извне в папке Wine и заражать флешки. Такие вирусы никаким образом не могут повредить Mint, а только компьютеры с Windows. Именно для этого и нужен антивирус в Mint, чтобы сохранять спокойный сон пользователей Windows. Итак, установим румынский антивирус — BitDefender.

Выполним в Терминале:

sudo sh -c 'echo "deb http://download.bitdefender.com/repos/deb/ bitdefender non-free" >> /etc/apt/sources.list.d/bitdefender.list'

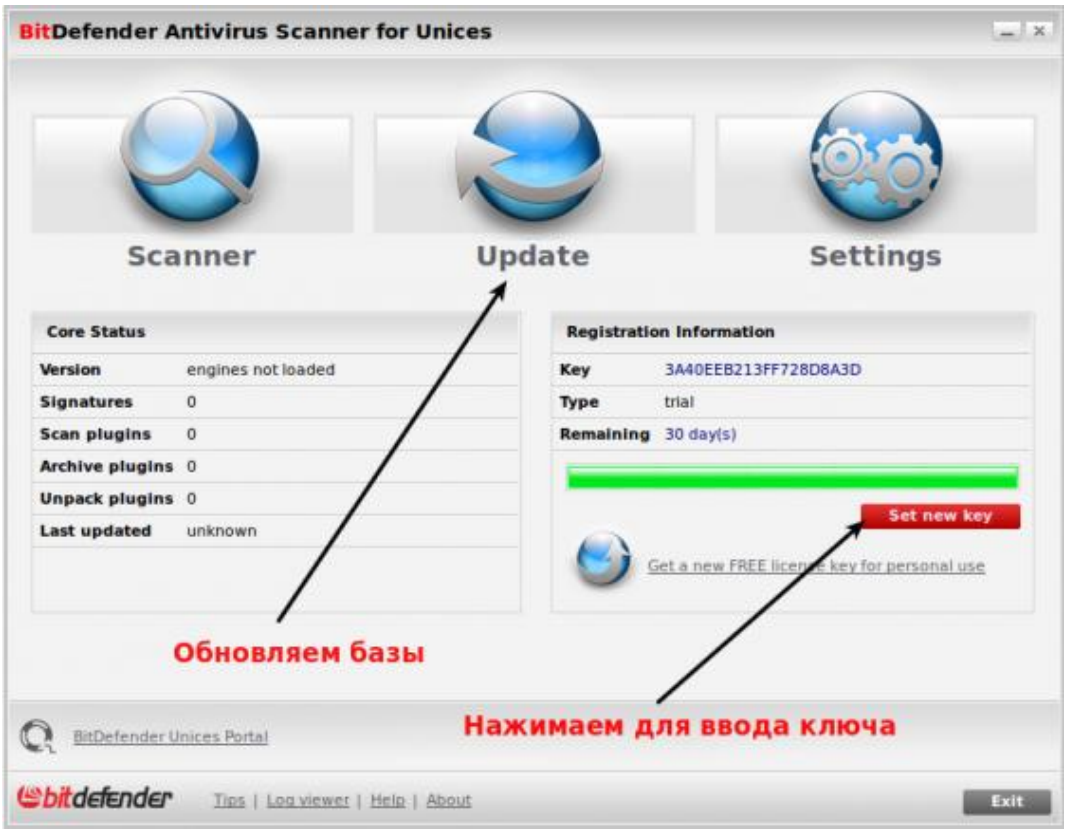
wget http://download.bitdefender.com/repos/deb/bd.key.asc

sudo apt-key add bd.key.asc

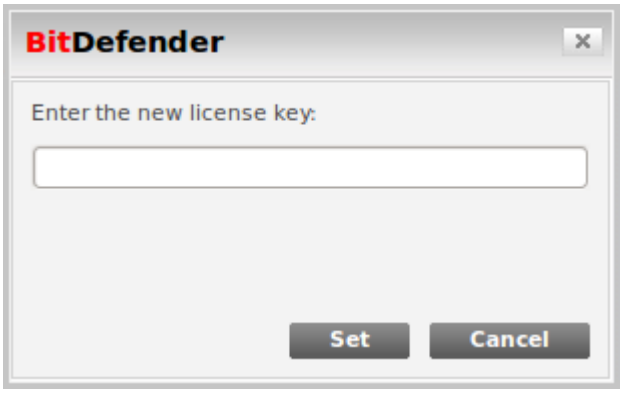
sudo apt-get update

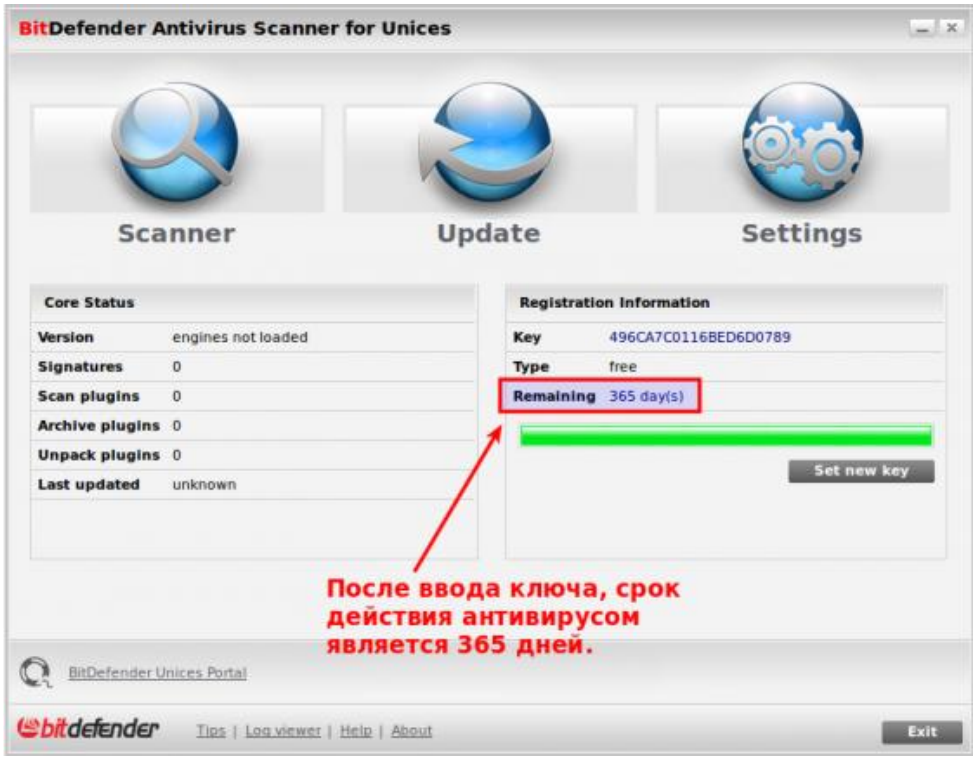
sudo apt-get install bitdefender-scanner-gui

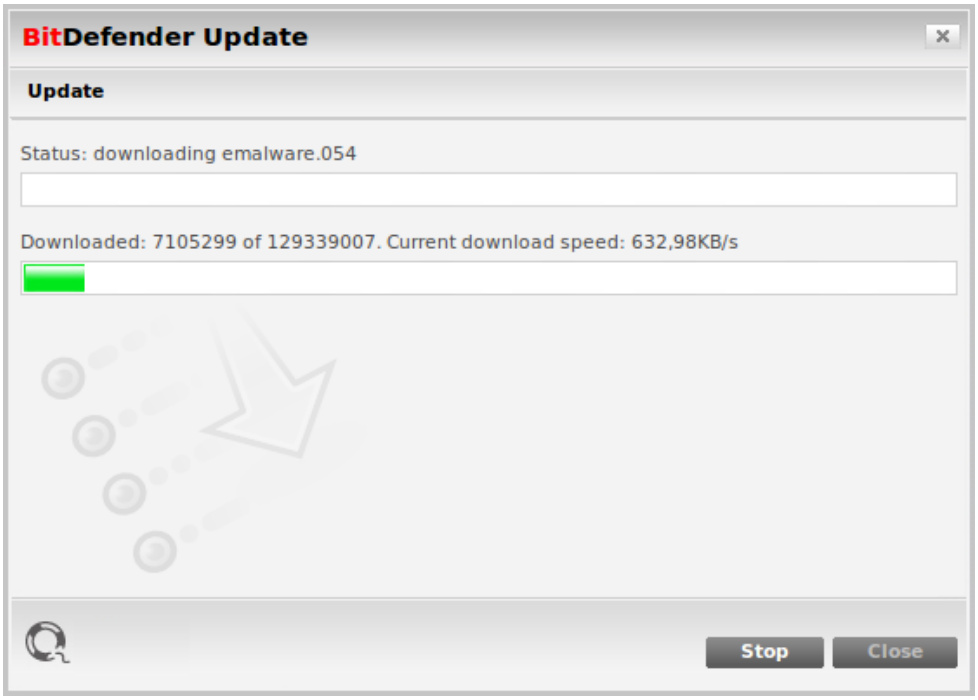
sudo reboot



После перезагрузки идем на страницу регистрации и регистрируемся. Естественно, что нужно указать реальный email, на который придет ключ для активации. Ожидаем некоторое время и проверяем свою почту. Находим там письмо с ключом и вводим в антиврус для активации.







Если будут проблемы после запуска сканера BitDefender, то решаем проблему так:

sudo touch /opt/BitDefender-scanner/var/lib/scan/bdcore.so.linux-x86_64

sudo ln -fs /opt/BitDefender-scanner/var/lib/scan/bdcore.so.linux-x86_64 /opt/BitDefender-scanner/var/lib/scan/bdcore.so

sudo bdscan --update

12.3. ПРОВЕРКА LINUX НА НАЛИЧИЕ РУТКИТОВ

Для того, чтобы своевременно обнаружить руткиты в ОС, есть замечательная утилита - **rkhunter**, которая осуществляет проверку вашей операционной системы по нескольким признакам, а именно по базе данных сигнатур, по открытым сетевым портам, по подложным копиям важных системных файлов и так далее.

В операционной системе Ubuntu это приложение входит в официальный репозиторий и есть возможность установить его одной командой:

```
sudo apt-get install rkhunter
```

Владельцы других дистрибутивов могут ознакомиться со способами установки на официальном сайте rkhunter.

Установка не должна занять много времени, после которой необходимо обновить базу данных сигнатур командой:

```
sudo rkhunter --update
```

Чтобы запустить проверку операционной системы, необходимо выполнить команду:

```
sudo rkhunter --check
```

По умолчанию после каждого теста нужно нажимать любую клавишу для того, чтобы успеть ознакомится с промежуточными результатами, если этого не требуется, то можно запустить проверку с ключом **--sk**:

```
sudo rkhunter --check --sk
```

Или вообще без вывода на экран какой-либо информации:

```
sudo rkhunter --check -q
```

12.3.1. Проверка серверов на наличие руткитов

Если проверка будет запускаться на сервере, то целесообразнее поставить задачу в планировщик **crontab**, чтобы каждый раз не делать это вручную. Для этого открываем список задач:

```
sudo crontab -e -u root
```

В конце файла добавляем новую запись:

```
0 0 * * * rkhunter --update
0 1 * * * rkhunter --check
```

Эта запись "говорит" планировщику, что обновление сигнатур будет происходить ежедневно в 23.59, а проверка системы в 01.00.

А для того, чтобы результаты проверки были всегда на виду, настраиваем ежедневное уведомление по электронной почте (работает, если на этом сервере уже настроен *postfix* или *exim*).

1. Для этого открываем конфигурационный файл */etc/rkhunter.conf*:

```
sudo nano /etc/rkhunter.conf
```

2. Добавляем значение параметру **MAIL-ON-WARNING**. Должно получиться, к примеру, так:

```
# NOTE: This option should be present in the configuration file.
#
#MAIL-ON-WARNING=me@mydomain root@mydomain
MAIL-ON-WARNING="admin@itshaman.ru"
```

После этого при обнаружении проникновения Вы будете "в курсе". *rkhunter* - это действенный способ проверки ОС на наличие руткитов.

12.4. БЕЗОПАСНОЕ УДАЛЕНИЕ ДАННЫХ В LINUX MINT

Как правило в Ubuntu/Linux Mint для удаления файлов служат команды в терминале: remove, purge. Или из файлового менеджера правый клик на файле и «Удалить». В обоих случаях файлы удаляются из системы, но их следы остаются на жёстком диске компьютера и при желании компетентный злоумышленник, укравший ваш компьютер или правоохранительные органы могут восстановить эти файлы, сколько бы раз они не были перезаписаны.

Если вы действительно хотите удалить файлы с жёсткого диска компьютера бесследно, то для этого нужно использовать более сложные команды.

В репозитории есть пакет под названием secure-delete - утилита для вычистки данных файлов, из свободного места на диске, подкачки и памяти.

Или для установки пакета Secure-Delete в Ubuntu/Linux Mint выполните команду в терминале:

```
sudo apt-get install secure-delete
```

Пакет Secure-Delete поставляется с четырьмя командами:

srm - используется для удаления файлов или каталогов (папок) на жестком диске;
smem - используется стереть следы данных из памяти компьютера (RAM);
sfill - используется стереть все следы данных свободного пространства на жестком диске;
sswap - используется стереть все следы данных из раздела подкачки.

Команда SRM предназначена для удаления данных с компьютера в безопасном режиме, которые не могут быть восстановлены с помощью воров и правоохранительных органов.

Примеры использования SRM:

1. Удаление файлов с помощью SRM из директории tmp

srm /tmp/myfile.txt

Замените myfile.txt на собственное название текстового файла.

2. Удаление с помощью SRM каталогов (папок) из директории tmp

srm -r /tmp/mydir/

Замените mydir на собственное название папки, которую хотите удалить.