

**УТВЕРЖДАЮ**

Начальник 27 кафедры

ПОЛКОВНИК

С. Войцеховский

« \_\_\_\_ » \_\_\_\_\_ 2022 г.

Практическое занятие № 13  
по учебной дисциплине  
«Защита информации»  
на тему:

**«Работа с антивирусным комплексом DrWeb для ОС MSVC 3.0»**

Рассмотрено и одобрено  
на заседании кафедры № 27

« \_\_\_\_ » \_\_\_\_\_ 202\_ г. протокол № \_\_\_\_

Санкт-Петербург  
2022

## **I. ТЕМА И ЦЕЛЬ ПРАКТИЧЕСКОГО ЗАНЯТИЯ**

**Тема занятия:** Работа с антивирусным комплексом DrWeb для ОС  
МСВС 3.0

1. Научиться установке антивирусного комплекса DrWeb на ПЭВМ.
2. Научиться обновлять антивирусные базы ПЭВМ с магнитных носителей.

Время - 90 мин

Место - класс ПЭВМ

**Учебно-материальное обеспечение**

1. ПЭВМ
2. Дистрибутив ОС МСВС 3.0, DrWeb

### **1.УЧЕБНЫЕ ВОПРОСЫ И РАСЧЕТ ВРЕМЕНИ**

№ п.п.	Учебные вопросы	Время, мин
1	2	3
1.	Вступительная часть	5
2.	Проверка готовности слушателей к занятию	
	Учебные вопросы	
	1. Установка антивирусного комплекса DrWeb на ПЭВМ.	55
	2. Обновление антивирусных баз ПЭВМ с магнитных носителей.	25
3.	Заключительная часть	5
	Задание и методические указания слушателям на самостоятельную подготовку	

## **II. УЧЕБНЫЕ МАТЕРИАЛЫ**

Вступительная часть

Товарищи слушатели, в ходе предыдущего практического занятия вы научились работе с дисками и файловой системой ОС МСВС, администрировать ОС МСВС 3.0. при помощи штатных механизмов.

Целью сегодняшнего занятия является - приобретение первоначальных практических первоначальных практических навыков в установке антивирусного комплекса DrWeb на ПЭВМ, научиться обновлять антивирусные базы ПЭВМ с магнитных носителей.

Итак, тема сегодняшнего практического занятия - " Работа с антивирусным комплексом DrWeb для ОС МСВС 3.0 ".

Для достижения поставленных учебных целей вам требуется отработать два учебных вопроса занятия:

1. Установка антивирусного комплекса DrWeb на ПЭВМ.

## 2. Обновление антивирусных баз ПЭВМ с магнитных носителей.

Порядок проведения занятия будет следующий - сначала вы ответите на ряд контрольных вопросов, что позволит оценить вашу теоретическую готовность к занятию, а затем в рамках рассматриваемых вопросов занятия вы будете исполнять задания с использованием ПЭВМ. Ваша работа будет оцениваться на местах.

### Контрольные вопросы до начала занятия.

Вопрос № 1: Сколько логических дисков может быть проинициализировано на одном жестком диске в ОС MSVC?

Ответ: 4.

Вопрос № 2: Что такое скрипт?

Ответ: *скрипт* – небольшая программа на специальном языке, которая с помощью запрограммированных команд выполняет соответствующую последовательность действий

Вопрос № 3: Дайте определение понятию «**файловая система**». Какая ФС используется в ОС MSVC?

Ответ: **Файловая система** – это методы и структуры данных, которые используют ся операционной системой для хранения файлов на диске или его разделе. Для ОС MSVC 3.0 доступны при установке две файловые системы: Ext2 FS и Ext3 FS.

**Выполнение практического занятия проводится в соответствии с заданием на практическое занятие № 13, приведенного в Приложении.**

### Контрольные вопросы

1. С помощью какой команды можно создать *пользователя* в консольном режиме?

2. С помощью какой команды можно создать *группу пользователей* в консольном режиме?

3. С помощью какой команды можно временно получить доступ к системе с правами *суперпользователя*?

4. С помощью каких команд в консольном режиме осуществляется удаление пользователей и групп пользователей?

5. С помощью каких команд в консольном режиме осуществляются перезагрузка и завершение работы системы?

6. Назовите имя главного конфигурационного файла программы-сканера Dr.Web?

7. Как называется и где находится лог-файл программы Dr.Web?

8. Что такое *скрипт*?

9. В каком месте на диске хранятся сигнатуры вирусных баз программы Dr.Web?

10. Какие антивирусные комплексы вам знакомы? Перечислите наиболее известные сертифицированные продукты.

11. Каков принцип работы антивирусных средств?
12. Дайте определение компьютерного вируса.

### **Заключительная часть**

Товарищи слушатели, на сегодняшнем занятии вы практически отработали вопросы с установкой и обновлением антивирусных баз антивирусного комплекса DrWeb.

На занятии активно и правильно выполняли задания слушатели: \_\_\_им выставлены оценки. На следующем занятии вы перейдете к изучению темы 3 «Особенности построения современного математического обеспечения ЭВМ»

**Задание и методические указания слушателям на самостоятельную подготовку**

1. Изучить Руководство администратора Dr.Web для интернет-шлюзов UNIX (ОС MCBC 3.0).

## **Задание на практическое занятие № 13**

### **«Работа с антивирусным комплексом Doctor Web для MCBC 3.0»**

**Цели работы:** выработать практические умения и приобрести практические навыки по:

1. созданию пользователей и групп пользователей
2. установке антивирусного комплекса на ПЭВМ.
3. обнаружению и удалению компьютерных вирусов (тестовых) с ПЭВМ.
4. обновлению антивирусных баз ПЭВМ с магнитных носителей.

---

#### **1. Задание на практическое занятие**

---

- 1.0** Научиться корректно завершать работу с ОС. Создавать и удалять пользователей и группы пользователей.
- 1.1.** Изучить документ «Руководство оператора объекта ВТ «Антивирусная программа DrWeb для ОС MCBC 3.0».
- 1.2.** Установить антивирусный комплекс Doctor Web для ОС MCBC 3.0 на ПЭВМ.
- 1.3.** Обнаружить и удалить компьютерные вирусы (тестовые) с ПЭВМ.
- 1.4.** Обновить антивирусные базы ПЭВМ с магнитных носителей.
- 1.5.** Написать скрипт для автоматизации процесса проверки папки...(указывает преподаватель) на наличие компьютерных вирусов и вывода отчёта о ходе проверки на экран монитора (запускать скрипт с помощью кнопки на рабочем столе).

---

#### **2. Подготовка к работе**

---

Подготовка к работе проводится в часы самоподготовки. В ходе её каждый слушатель обязан:

- 2.1.** Изучить настоящее задание.
- 2.2.** Изучить руководство оператора объекта ВТ «Антивирусная программа DrWeb для ОС MCBC 3.0»

---

#### **3. Методические указания**

---

**3.1.** В классе ПЭВМ слушатели самостоятельно под руководством преподавателя выполняют п. 4 настоящего задания.

**3.2.** При выполнении задания работу следует спланировать таким образом, чтобы в первую очередь изучить руководство оператора объекта ВТ «Антивирусная программа DrWeb для ОС MCBC 3.0», а затем приступить к использованию «Антивирусной программы DrWeb для ОС MCBC 3.0»

**3.3.** В ходе практической работы запрещается вносить изменения, удалять или добавлять какие-либо компоненты, настройки и параметры операционной системы.

---

## 4. Выполнение работы

---

### ЗАДАНИЕ 1. Вход в систему, перезагрузка и выключение ОС в консольном режиме. Управление пользователями и группами пользователей

#### 1.1 Вход в ОС MCBC 3.0

Действия администратора при первом входе в ОС MCBC. После того как в ответ на приглашение буден введен login: **root**, а также его пароль (**11111111**), вы осуществите первый вход в систему (рис. 1).

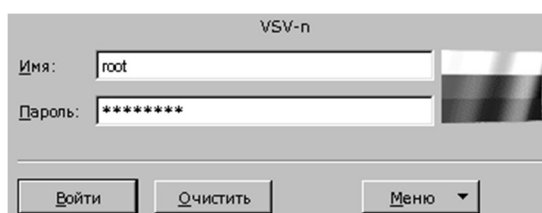


Рис. 1. Окно входа в ОС MCBC 3.0

#### 1.2 Создание пользователей в консольном режиме

Откройте консоль, пройдя последовательно по вкладкам ПУСК – ПРОГРАММЫ – УТИЛИТЫ – ELK ТЕРМИНАЛ (можно использовать любой терминал) (рис. 2).

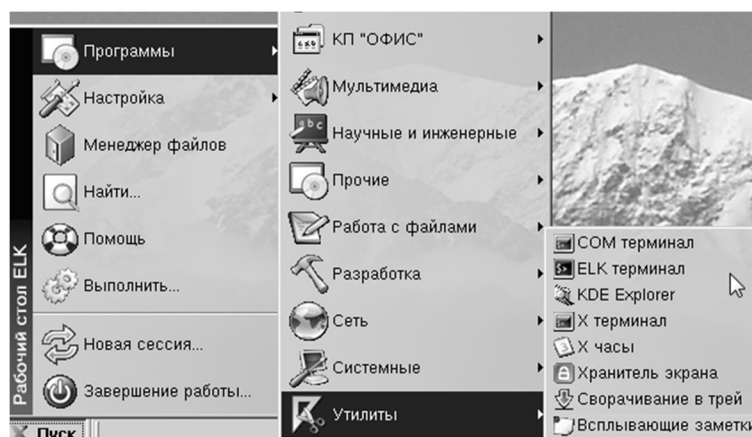


Рис.2. Порядок запуска программы **ELK терминал**

Откроется консоль. Вы увидите примерно такую надпись:

**[root@VSV-n root]#**

Такая строка называется *приглашением*. Появление приглашения означает, что система готова воспринять и выполнить вашу команду.

Прежде чем предложить вам ввести первую команду, надо сказать, что в любой UNIX-системе учитывается регистр символов, т.е. различаются строчные и прописные буквы. Поэтому вводить все команды и их параметры следует именно так, как указано в примерах, учитывая регистр.

В консольном режиме пользователя можно создать с помощью команды **useradd**. После имени команды надо ввести пробел и имя пользователя, например, **Ivan**:

```
[root]# useradd Ivan
```

После этого система будет знать о существовании пользователя Ivan (говорят, будет «открыт счет для пользователя Ivan»).

Однако войти в систему («легироваться») под этим именем еще невозможно. Для того чтобы система разрешила работать пользователю с именем Ivan, надо задать ему пароль. Для этого вводим команду **passwd**

```
[root]# passwd Ivan
```

Появится строка

**Новый UNIX пароль:**

Вводите пароль (не менее 8 символов). После того как вы завершите ввод нажатием клавиши <Enter>, система попросит ввести его повторно:

**Наберите новый UNIX пароль еще раз:**

Если вы не ошиблись при вводе, (пароль приходится вводить «вслепую», поскольку он не отображается на экране) появится сообщение и приглашение системы:

**passwd: все данные об аутентификации успешно обновлены**  
(all authentication tokens updated successfully).

Если вы выбрали пароль не удачно (слишком короткий или простой), вам будет выдано предупреждение (рис. 3) (**Неверный пароль: it does not enough DIFFERENT characters**), но система все равно примет пароль и позволит новому пользователю входить с ним в систему.

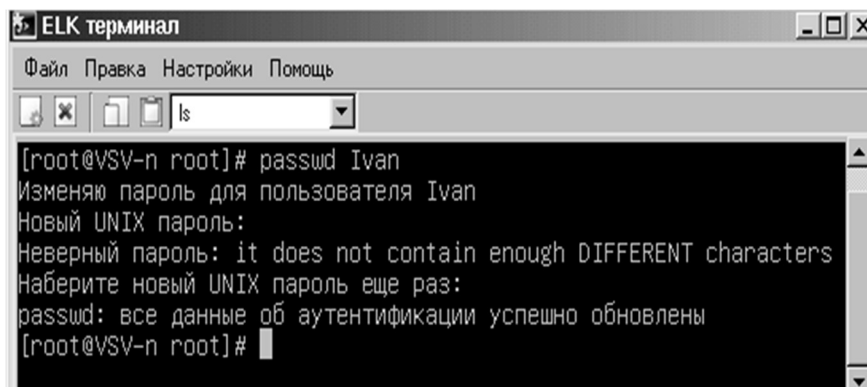
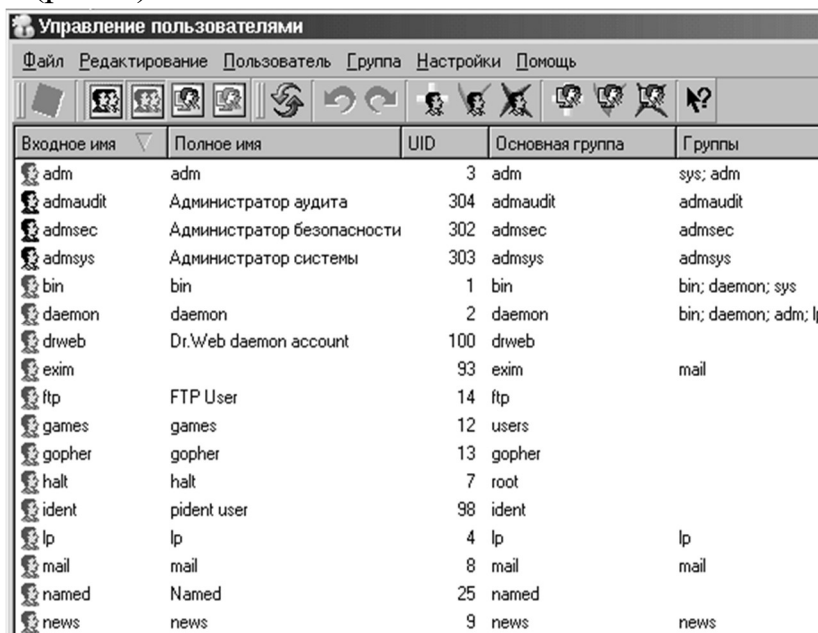


Рис. 3. Создание пользователя в консоли **ELK терминал**

### 1.3 Создание (удаление) пользователей и групп пользователей в графическом режиме

Для этого необходимо использовать программу **Управление пользователями**. Для ее запуска необходимо последовательно открыть следующие вкладки: **Пуск – Настройка – Панель управления ELK – Безопасность – Пользователи** (рис. 4).



Входное имя	Полное имя	UID	Основная группа	Группы
adm	adm	3	adm	sys; adm
admaudit	Администратор аудита	304	admaudit	admaudit
admsec	Администратор безопасности	302	admsec	admsec
admsys	Администратор системы	303	admsys	admsys
bin	bin	1	bin	bin; daemon; sys
daemon	daemon	2	daemon	bin; daemon; adm; lp
drweb	Dr.Web daemon account	100	drweb	
exim	exim	93	exim	mail
ftp	FTP User	14	ftp	
games	games	12	users	
gopher	gopher	13	gopher	
halt	halt	7	root	
ident	pident user	98	ident	
lp	lp	4	lp	lp
mail	mail	8	mail	mail
named	Named	25	named	
news	news	9	news	news

Рис. 4. Главное окно программы **Управление пользователями**

Перейдите на вкладку **Пользователь** и из выпадающего меню выберите команду **Добавить**. Запустится окно создания нового пользователя.

В первом окне введите имя пользователя и нажмите кнопку **Далее**.

Во втором окне введите пароль пользователя (не менее восьми символов), подтвердите его и нажмите кнопку **Далее**.

В третьем окне установите атрибуты безопасности пользователя максимальным уровнем **несекретно** и нажмите кнопку **Далее**.

В четвертом окне, предназначенном для ввода фотографии пользователя, нажмите кнопку **Готово**.

Перейдите на вкладку **Файл** и из выпадающего меню выберите команду **Сохранить**. Для выхода из программы **Управление пользователями** перейдите на вкладку **Файл** и из выпадающего меню выберите команду **Выход**.

Теперь вы можете закончить сессию под учетной записью текущего пользователя и войти под учетной записью нового пользователя. Для этого пройдите последовательно по вкладкам: **Пуск – Завершение работы – Закончить сессию**.



### 1.4 Создание группы пользователей АА в консольном режиме.

Каждый пользователь может быть включен в произвольное число групп. Включение пользователя в различные группы может быть осуществлено путем «ручного» редактирования файла **/etc/group** суперпользователем, а может быть выполнено с помощью команд **groupadd** и **groupmod**.

Для создания группы пользователей АА в консольном режиме откройте консоль, пройдя последовательно по вкладкам ПУСК – ПРОГРАММЫ – УТИЛИТЫ – ELK ТЕРМИНАЛ (можно использовать любой терминал) (см. рис. 2). Откроется консоль (см. рис. 3).

В консольном режиме группу пользователей АА можно создать с помощью команды **groupadd**. После имени команды надо ввести пробел и имя группы пользователей, например, АА (рис. 5):

```
[root]# groupadd АА
```



Рис. 5. Создание группы пользователей АА  
в консоли **ELK терминал**

Группа пользователей АА создана.

### 1.5 Создание группы пользователей АА в графическом режиме

Для создания группы пользователей необходимо использовать программу **Управление пользователями**. Для ее запуска необходимо последовательно открыть следующие вкладки: **Пуск – Настройка – Панель управления ELK – Безопасность – Пользователи** (см. рис. 4).

Перейдите на вкладку **Группа** и из выпадающего меню выберите команду **Добавить**. Запустится окно создания новой группы пользователей. Введите имя группы пользователей **АА**, при необходимости добавьте необходимых пользователей в создаваемую группу и нажмите кнопку **Готово**.

Перейдите на вкладку **Файл** и из выпадающего меню выберите команду **Сохранить**. Для выхода из программы **Управление пользователями** перейдите на вкладку **Файл** и из выпадающего меню выберите команду **Выход**. Группа пользователей АА создана.

### 1.6 Команда usermod

Команда **usermod** имеет те же опции, что и **useradd**, только используется для изменения параметров существующего пользователя, причем на момент

применения этой команды суперпользователем данный пользователь не должен быть легирован в системе.

### 1.7 Команды **su**, **sg**, **exit** и **man**

В процессе работы пользователь может сменить имя, с которым он вошел в систему (поработать в системе от имени другого пользователя). Для этого используется команда **su**. Команда **su** чаще всего используется для того, чтобы временно получить доступ к системе с правами суперпользователя. Параметр в этом случае указывать не требуется.

После того как вы поработали под чужим именем, достаточно выполнить команду **exit**, чтобы вернуть себе свое обычное имя. Команда **sg** аналогична команде **su**, но используется для смены группы. Доступ предоставляется в том случае, если пользователь является членом указанной группы.

Команда **man** — это система встроенной помощи Linux (MCBC 3.0). Вводить ее надо с параметром — именем другой команды или ключевым словом, например,

```
[root]# man passwd
```

В ответ вы получите описание соответствующей команды или информацию по теме, обозначенной ключевым словом. Поскольку информация обычно не помещается на одном экране, при просмотре можно пользоваться клавишами <PageUp> и <PageDown>, а также клавишей пробела. Нажатие клавиши <Q> в любой момент приводит к выходу из режима просмотра и возврату в режим ввода команд.

### 1.8 Удаление пользователей и групп пользователей

Удаление пользователей и связанных с ним файлов осуществляется командой **userdel**.

Удаление группы пользователей осуществляется командой **groupdel**.

Для создания (удаления) пользователей и групп пользователей в графическом режиме необходимо использовать программу **Управление пользователями** (см. рис. 6.4). Для ее запуска необходимо последовательно открыть следующие вкладки: **Пуск – Настройка – Панель управления ELK – Пользователи**.

### 1.9 Перезагрузка и завершение работы системы

Работая с ОС MCBC 3.0, следует быть аккуратным при выходе из системы. Нельзя просто выключить компьютер, т.к. ОС MCBC 3.0 имеет журналируемую файловую систему, изменения в которую вносятся не оперативно, а через определенные промежутки времени, при отключении питания информация может быть потеряна, а файловая система повреждена.

1.9.1 Перезагрузку можно выполнить несколькими способами:

дать команду **shutdown -r**;

использовать команду **reboot**.

### 1.9.2 Завершение сеанса работы

По окончании работы пользователь завершает работу с интерпретатором, вводя команду **exit** или **logout**. Операционная система при этом завершает сеанс пользователя.

1.9.3 Пользователь может инициализировать завершение работы системы нажатием комбинации клавиш **Ctrl+Alt+Del**, если в файле `/etc/inittab` включена строка, показанная ниже:

**ca::ctrlaltdel:/sbin/shutdown -t3 -h now**

1.9.4 Для завершения работы системы можно использовать еще ряд команд: **halt**, **reboot**, **shutdown** и **poweroff**. Эти команды могут быть вызваны только пользователями, которым дано на это право, т.е. *администраторами*.

1.9.5 Команда **shutdown** – самый безопасный и наиболее корректный способ инициирования остановки или перезагрузки системы, либо возврата в однопользовательский режим.

Общая форма вызова команды **shutdown** следующая:

**shutdown [-t секунд] [опции] время [сообщение для пользователей].**

Можно дать указание *shutdown делать паузу перед остановом системы*. Во время ожидания **shutdown** посылает зарегистрированным пользователям через постепенно укорачивающиеся промежутки времени сообщения, предупреждая их о приближающемся останове. По умолчанию в сообщениях просто говорится о том, что *система заканчивает работу*, и указывается время, оставшееся до остановки. При желании администратор может добавить собственное короткое сообщение, в котором содержится информация о том, почему система останавливается, и сколько примерно времени придется подождать, прежде чем пользователи вновь смогут войти в систему.

Команда **shutdown** позволяет указать, *что конкретно должна сделать машина*: остановиться, перейти в однопользовательский режим или перезагрузиться.

Синтаксис команды:

**shutdown [flags] time [warning-message]**

[warning-message] – сообщение, посылаемое всем пользователям, в настоящий момент зарегистрированным в системе, а **time** представляет собой время выполнения отключения системы. Оно может быть указано в нескольких форматах.

Время может быть указано как абсолютное время в формате **hh:mm**, где **hh** – час (одна или две цифры), а **mm** – минуты (две цифры). Опции команды **shutdown**, представлены в табл. 1.

Таблица 1. Опции командной строки команды shutdown

Опции	Описание
-r	Заставляет программу <b>init</b> перезагрузить систему после остановки всех процессов
-h	Останавливает систему после остановки всех процессов
-k	Не останавливает систему, а только посылает предупреждающее сообщение пользователям
-c	Отменяет выполнение запущенного процесса <b>shutdown</b>
-t секунд	Заставляет программу <b>init</b> подождать указанное количество секунд, прежде чем посылать процессам сигналы <b>SIGTERM</b> и <b>SIGKILL</b>
-f	Пропустить проверку файловых систем при перезагрузке
-F	Обязательно выполнять проверку файловых систем при перезагрузке
время	Время начала остановки. Время можно указывать в формате чч:мм или в формате +N, где N – количество минут после текущего момента. Можно также указывать значение <b>now</b> , являющееся псевдонимом +0 минут
Сообщение для пользователей	Можно также посылать пользователям сообщение с помощью команды <b>wall</b>

## ЗАДАНИЕ 2. Установка антивирусного комплекса Dr.Web для ОС MCBC 3.0 на ПЭВМ

### 2.1 Процесс установки программы Dr.Web

Установка, обновление и удаление «Dr.Web для файловых серверов UNIX» могут быть осуществлены с помощью:

графических инсталлятора и деинсталлятора;  
консольных инсталляторов и деинсталляторов.

Дистрибутив программного комплекса «Dr.Web для файловых серверов UNIX» распространяется в виде самораспаковывающегося архива (Dr.Web-file-servers-5.\*.\*-linux.run).

Перейдите в каталог с дистрибутивом программы с помощью команды **cd**.

**cd /distrib**

В данном примере **/distrib** – каталог с дистрибутивом программы.

Для автоматической установки компонентов программного комплекса «Dr.Web для файловых серверов UNIX» разрешите исполнение архива, например, командой:

**# chmod +x Dr.Web-file-servers-5.0.0-linux.run**

и затем запустите его на исполнение командой:

## # ./Dr.Web-file-servers-5.0.0-linux.run

Или воспользуйтесь стандартным файловым менеджером вашей графической оболочки как для изменения свойств файла, так и для его запуска.

При этом будет создана директория `Dr.Web-file-servers-5.0.0-linux` с набором файлов внутри, и автоматически запустится графический инсталлятор. Если запуск был осуществлен не с правами администратора, то инсталлятор сам попытается повысить права.

При запуске графического инсталлятора открывается окно программы установки (рис. 6).

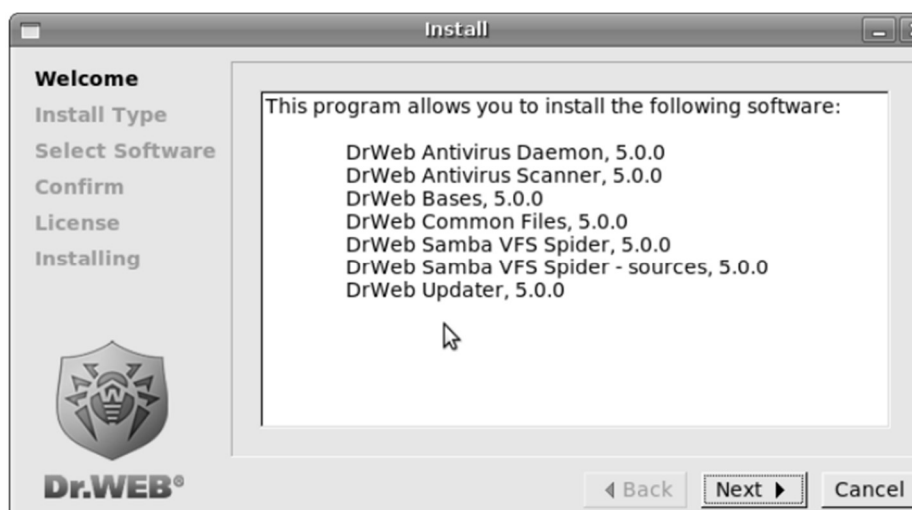


Рис. 6. Окно **Welcome** программы установки

Навигация осуществляется с помощью кнопок **Back** и **Next**. Установку можно прервать в любой момент, нажав кнопку **Cancel**.

В следующем окне **Install Type** вы можете выбрать тип установки: базовый **Dr.Web for File Servers** со всеми компонентами по умолчанию или пользовательский **Custom Configuration** (рис. 7).

Если вы выбрали пункт **Custom Configuration**, то следующим откроется окно **Select Software**, в котором вы сможете указать необходимые вам компоненты.

Обратите внимание, что если для установки выбранного вами компонента должен быть предварительно установлен другой компонент, то соответствующая зависимость будет отмечена автоматически.

Таким образом, если вы установите флажок напротив **Dr.Web Antivirus Daemon**, то флажки автоматически появятся напротив пунктов **Dr.Web Bases** и **Dr.Web Common Files**. Нажав на кнопку **Install All**, вы сможете отметить сразу все компоненты. Нажатие на кнопку **Install None** удалит все предоставленные флажки.



Рис. 7. Окно выбора типа установки

Нажмите на кнопку **Install All**. После завершения выбора компонентов (либо если на предыдущем этапе вы выбрали базовый тип установки) вы переходите к окну **Confirm**, в котором увидите все выбранные вами компоненты и сможете принять окончательное решение.

Затем вам нужно будет ознакомиться с текстом Лицензионного Договора и принять его, чтобы продолжить установку. Тексты Лицензионного Договора на английском и русском языках входят в комплект поставки (файлы **LICENSE** и **LICENSE.ru** соответственно).

В последнем окне **Installing** выводится отчет о процессе установки в режиме реального времени.

Нажав на кнопку **Close**, вы завершите установку программного комплекса **Dr.Web** для файловых серверов **UNIX**.

## 2.2 Лицензионный ключевой файл

Сразу после установки программа **Dr.Web** может быть запущена только в качестве ознакомительной версии. Для ее превращения в полнофункциональную необходимо получение регистрационного ключа от распространителя программы. Регистрационный ключ к сканеру **Dr.Web** для **MCBC 3.0** – это файл, поставляемый под именем **drweb32.key**. Его надлежит скопировать в каталог, в который установлена программа (по умолчанию **/opt/drweb**).

## ЗАДАНИЕ 3. Использование сканирующего модуля **Dr.Web**

### 3.1. Запуск программы-сканера

Сканер **Dr.Web** – программа с текстовым интерфейсом, функционирующая в консольном режиме (или в окне эмулятора терминала в **XWindow**). Ее запуск в **MCBC** осуществляется из каталога **/opt/drweb** последовательностью команд:

```
cd /opt/drweb
./drweb
```

или `/opt/drweb/drweb`

Сканер может быть запущен как от лица *администратора системы*, так и от лица обычного *пользователя*. Разумеется, в последнем случае проверка на вирусы будет выполняться только в тех каталогах, к которым пользователь имеет доступ с правом чтения, а лечение инфицированных файлов – в каталогах, в которых он имеет право записи (как правило, это домашний каталог пользователя, \$HOME). Кроме того, существуют и другие ограничения при запуске сканера в пользовательском режиме (например, на перемещение и переименование инфицированных файлов).

После запуска сканера на экран выводится заставка с названием программы и ее целевой платформы (**МСВС**), номером версии и датой ее выпуска, контактными координатами. Далее выводится сообщение о регистрационных данных пользователя и загрузке антивирусной базы данных, включая и ее обновления, если таковые были установлены (рис. 6.8).

```
[root@VSV-n drweb]# cd /opt/drweb
[root@VSV-n drweb]# ./drweb
Dr.Web (R) Scanner for Linux v4.44.0 (4.44.0.0801230)
Copyright (c) Igor Daniloff, 1992-2007
Doctor Web, Ltd., Moscow, Russia
Support service: http://support.drweb.com
To purchase: http://buy.drweb.com
Report dated 2012-10-29, 00:22:46
Command line:
Shell version: 4.44.0.10060 <API:2.2>
Engine version: 5.0.0.12182 <API:2.2>
Loading /var/drweb/bases/drwtoday.vdb - Ok, virus records: 4847
Loading /var/drweb/bases/drw50031.vdb - Ok, virus records: 5242
Loading /var/drweb/bases/drwrisky.vdb - Ok, virus records: 3316
Loading /var/drweb/bases/drwnasty.vdb - Ok, virus records: 19303
Total virus records: 577022
Key file: /opt/drweb/drweb32.key
License key number: 0014065672
License key activates: 2010-03-17
License key expires: 2013-12-31
-?, -help, -h, --help - display help
[root@VSV-n drweb]#
```

Рис. 6.8. Окно запуска сканера Dr.Web

(Пример листинга является условным, в реальности даты, номера версий и количество вирусных записей могут быть иными).

После этого возвращается приглашение командной оболочки. Все иные действия по обнаружению и обезвреживанию вирусов требуют применения опций командной строки.

Для сканера Dr.Web предусматриваются многочисленные опции командной строки.

Они отделяются от указания пути пробелом и предваряются символом - (дефис). Полный список опций можно получить, запустив программу Dr.Web со следующими опциями:

**-?** или **-help**

### 3.2 Опции командной строки

Основные опции программы могут быть сгруппированы следующим образом:

- опции области проверки;
- опции диагностики;
- опции действий;
- опции интерфейса.

Общий формат запуска программы следующий (предполагается, что текущим является каталог **/opt/drweb**):

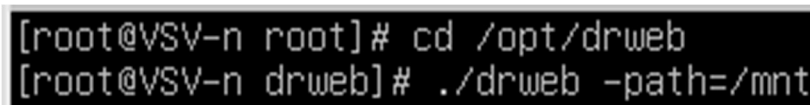
***./drweb -path=<путь> [опции],***

Где *путь* – путь к проверяемому каталогу или маска тестируемых файлов.

Например: ***cd /opt/drweb***

***./drweb -path=/tmp***

По этой команде осуществляется проверка директории **/tmp** (рис. 9).



```
[root@VSV-n root]# cd /opt/drweb
[root@VSV-n drweb]# ./drweb -path=/mnt
```

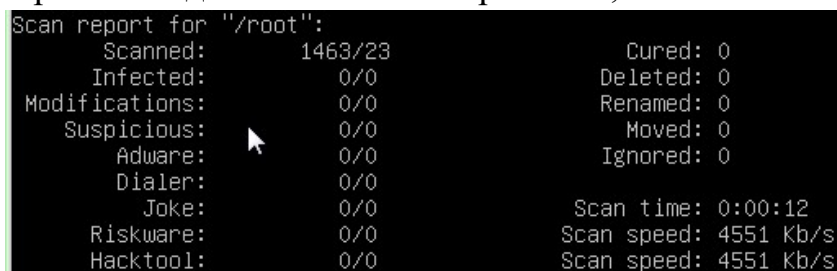
Рис. 9. Окно запуска программы-сканера drweb на проверку каталога **/tmp**

Запущенная без опций, только с указанием пути в качестве аргумента, программа-сканер осуществляет проверку указанного каталога, например домашнего каталога пользователя, используя набор опций по умолчанию.

В следующем примере проверяется домашний каталог пользователя:

***./drweb -path=~***

после чего программа выдает отчет о сканировании, показанный на рис. 10.



```
Scan report for "/root":
  Scanned:      1463/23          Cured: 0
  Infected:     0/0             Deleted: 0
  Modifications: 0/0             Renamed: 0
  Suspicious:   0/0             Moved: 0
  Adware:       0/0             Ignored: 0
  Dialer:       0/0
  Joke:          0/0             Scan time: 0:00:12
  Riskware:     0/0             Scan speed: 4551 Kb/s
  Hacktool:     0/0             Scan speed: 4551 Kb/s
```

Рис. 10. Вид окна отчета программы-сканера drweb

Числа, разделенные символом **/**, означают: первое – общее количество файлов, второе – файлов в архивах. Кроме того, при обнаружении файлов, инфицированных известными вирусами, или файлов, подозрительных в этом



отношении, перед суммарным отчетом появляются соответствующие строки, имеющие примерно следующий вид:

*/path/file* инфицирован [*вирусом*] *ИМЯ\_ВИРУСА*

1. **Опции области проверки** указывают, где следует проводить проверку на вирусы.

**sd** – рекурсивный поиск и тестирование файлов в подкаталогах, начиная с текущего;

**fl** – следовать ссылкам, как для файлов, так и для каталогов; при этом ссылки, приводящие к заикливаю, игнорируются.

2. **Опции диагностики**, определяющие, какие типы объектов должны проверяться на вирусы, включают:

**ar** [d|m|r][n] – проверка файлов в архивах (ARJ, CAB, GZIP, RAR, TAR, ZIP), где d – удаление, m – перемещение, r – переименование архивов, содержащих инфицированные объекты; n – отключение вывода имен архиваторов;

**ml** [d|m|r][n] – проверка файлов почтовых программ;

**up** [n] – проверка исполняемых файлов, упакованных LZEXE, DIET, PKLITE, EXEPACK; n – отключение вывода имен утилит упаковки;

**fm** – диагностика файлов с внутренней структурой программных модулей;

**ha** – эвристический анализ файлов, поиск неизвестных вирусов.

3. **Опции действия** определяют, какие манипуляции должны быть выполнены в отношении инфицированных (или подозреваемых в этом) файлов. Они следующие:

**cu** [d|m|r] – лечение инфицированных файлов; дополнительные опции предписывают: d – удаление, m – перемещение, r – переименование инфицированных файлов;

**ic** [d|m|r] – определяет действия для неизлечимых файлов: d – удаление, m – перемещение, r – переименование неизлечимых файлов;

**sp** [d|m|r] – определяет действия для подозрительных файлов: d – удаление, m – перемещение, r – переименование подозрительных файлов. Опция перемещения **spm** переместит зараженный (или подозрительный на вирус) файл в предназначенный для этого каталог (по умолчанию, */var/Dr.Web/infected*).

4. **Опции интерфейса** определяют условия вывода результатов работы программы.

Некоторые из опций отменяют соответствующее им действие, если оканчиваются символом - (дефис). К ним принадлежат:

**-ar -cu -ha -ic -fl -ml -ok -sd -sp -up**

Например, при запуске сканера в форме

***drweb -path=<путь> -ha-***

проверка на вирусы будет производиться без эвристического анализа файлов, который обычно по умолчанию включен.

По умолчанию программа-сканер запускается с опциями:

***-ar -fm -ha -fl- -ml -sd -up***

Форма запуска сканера для повседневного использования представляется следующей:

***drweb -path=<путь> -cu -icd -spm -ar -fm -ha -fl -ml -sd -up***

### **3.3 Конфигурирование программы-сканера с помощью файла drweb.ini**

Вполне возможно использование сканера с настройками по умолчанию, но значительно удобнее настроить его для соответствия вашим требованиям и условиям эксплуатации. Настройки сканера хранятся в конфигурационном файле программы, по умолчанию его имя **drweb.ini**, размещается он в каталоге **/etc/drweb**. Конфигурационный файл **drweb.ini** состоит из трех разделов:

[Daemon];

[Scanner];

[Updater].

**Перейдите в раздел [Scanner] и внесите в него следующие изменения:**

#### **1. LogFilename={путь}**

Поставьте знак комментария (#) напротив строки LogFilename = syslog.

Создайте под ней новую строку:

**LogFilename = /var/drweb.ini/log/drweb.ini.log**

#### **2. HeuristicAnalysis = {Yes | No}**

Включение/выключение использования эвристического анализатора, который может находить неизвестные вирусы. Включение эвристического анализа делает возможным обнаружение неизвестных вирусов по априорным соображениям об устройстве вирусного кода. Особенностью этого типа поиска вирусов является приблизительный, вероятностный характер обнаружения заражения, что позволяет говорить не о зараженных, а лишь о подозрительных объектах.

Значение по умолчанию: **No**.

**ИЗМЕНИТЕ НА: YES**

#### **3. InfectedFiles = {реакция}**

Задаёт реакцию программы на обнаружение файла, инфицированного известным вирусом.

Допустимые значения параметра:

Report – только вывести информацию в отчет

Cure – попытаться вылечить объект

Delete – удалить зараженный файл

Move – переместить файл в каталог, заданный параметром Move Files To

Rename – переименовать файл, используя маску, заданную параметром Rename Files To

Значение по умолчанию - **Report. ИЗМЕНИТЕ НА: CURE**

**4. LogScanned = {Yes | No}**

Вывод в файл отчета информации обо всех проверяемых объектах, независимо от того, обнаружены вирусы или нет. Информация о том, что это не вирус, не информативна.

Значение по умолчанию: LogScanned = **Yes**                      **ИЗМЕНИТЕ НА: NO**

### **3.4 Информация по командам для архива, контейнера или почтового ящика**

Удаление, перемещение и переименование, заданное в связи с обнаружением зараженных объектов в архивах, контейнерах и почтовых ящиках, применяется к соответствующему архиву, контейнеру или почтовому ящику целиком. Имеется целый ряд аналогичных параметров, задающих реакцию программы на обнаружение тех или иных объектов:

**SuspiciousFiles** – возможно, файл заражен неизвестным вирусом.

**IncurableFiles** – файл заражен и не может быть *вылечен* (имеет смысл, только если InfectedFiles = Cure).

**ActionInfectedMail** – сообщение или почтовый ящик содержат инфицированный объект.

**ActionInfectedArchive** – архив (ZIP, TAR, RAR и другие) содержит инфицированный файл.

**ActionInfectedContainer** – контейнер (OLE, HTML, PowerPoint и другие) содержит инфицированный объект.

**ActionAdware** – файл содержит программу для показа рекламы (так называемое AdWare).

**ActionDialers** – файл содержит программу автоматического дозвона, обычно используется «сайтами для взрослых».

**ActionJokes** – файл содержит программу-шутку, которая может пугать или раздражать пользователя.

**ActionRiskware** – файл содержит опасную программу, которая может быть использована, в том числе, и злоумышленниками.

**ActionHacktools** – файл содержит программу, которая используется для взлома компьютеров и прочей вычислительной техники.

Для всех этих параметров предусмотрены те же возможные значения, что и для параметра InfectedFiles, кроме Cure. Дополнительно предусмотрено

действие Ignore, для консольной версии это действие схоже с действием Report, но код возврата не содержит данных о таких объектах.

Значение по умолчанию для каждого параметра: **Report**.

#### ЗАДАНИЕ 4. Обнаружение и удаление тестовых вирусов с ПЭВМ

1. Следует обратить внимание, что в состав дистрибутива программы Dr.Web входит специальный тестовый файл

*readme.eicar.rus*

С помощью текстового редактора из него легко изготовить программу *ecar.com* (см. указания об этом внутри самого файла), которая ведет себя подобно вирусу, вызывая сообщение вида:

/path/clients/drweb/ecar.com инфицирован Eicar Test File (Not a Virus!)

2. Файл *ecar.com* содержит:

X50!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*

Если создать файл (\*.com) и записать в него эти строки, то он кажется лишь модификацией файла *ecar.com*.

Этот файл не является вирусом, но обычно используется для того, чтобы протестировать реакцию антивируса на наличие вируса. С этой целью все современные антивирусные программы включают информацию о нем в свои вирусные базы.

3. **Задание.** Скопируйте файл *ecar.com* в проверяемый каталог (из дистрибутива Dr.Web выданного преподавателем или воспользуйтесь документацией к программе Dr.Web расположенной /opt/drweb/doc/.

4. Или создайте его сами, например: командой

*cat > /home/ecar.com* или в любом текстовом редакторе.

Осуществите проверку данного каталога программой Dr.Web. Убедитесь в том, что тестовый файл обнаружен программой Dr.Web (рис.11).

Убедитесь в том, что результаты проверки теперь (после выполнения п. 3.3.1) сохраняются в файле /var/drweb/log/drweb.log.

Каждый раз набирать перечень вышеперечисленных команд в командной строке неактуально, поэтому необходимо самостоятельно написать простейший скрипт (см. *материалы лекций*) и связать его с кнопкой для автоматического запуска.

Для его создания можно воспользоваться командой **cat**. В конце скрипта следует указать команду **sleep 25**, для того чтобы успеть просмотреть результаты санирования в терминале за 25 секунд. При необходимости время просмотра можно увеличить.

```
>/tmp/vsv_distrib_21=C4_10=CD=C5=D3_12=C7.tgz/gzipped.gz - archive TAR
/tmp/eicar.com infected with EICAR Test File (NOT a Virus!)

Scan report for "/tmp":
  Scanned:      797/653          Cured: 0
  Infected:     1/0             Deleted: 0
  Modifications: 0/0             Renamed: 0
  Suspicious:   0/0             Moved: 0
  Adware:       0/0             Ignored: 0
  Dialer:       0/0
  Joke:         0/0             Scan time: 0:00:07
  Riskware:     0/0             Scan speed: 48115 Kb/s
  Hacktool:     0/0             Scan speed: 48115 Kb/s
```

Рис. 11. Окно обнаружения  
тестового файла eicar.com программой Dr.Web

### ЗАДАНИЕ 5. Создание скрипта

Для того чтобы вы или другие пользователи могли через созданную вами кнопку запускать созданный вами скрипт, текстовый (пока) файл нужно сделать **исполняемым**. Это можно сделать несколькими способами:

в консоли с помощью выполнения команды:

**chmod a+x /«путь к скрипту»**

с помощью программы **тс**: для этого в программе **тс** перейти на вкладку **Файл** далее **Права доступа** и установите опции: **Запуск/поиск для владельца**, **Запуск/поиск для других** (если вы хотите, чтобы его запускали все пользователи компьютера). Рядом с файлом появится знак \*, а сам файл теперь будет **зеленого** цвета – станет **исполняемым**.

### Задание 6. Автоматический запуск программы DrWeb по нажатию кнопки

Для создания кнопки (ярлыка вашего скрипта) на рабочем столе необходимо:

Щелкнуть правой кнопкой мыши на рабочем столе, в контекстном меню выбрать пункт **Создать** и далее **Ярлык**. В окне, появившемся на вкладке **Основные поля**, укажите основные параметры вашей кнопки: в окне **\*имя** – имя кнопки (например: Dr.Web), в окне **тип** – **Приложение**, поле в окне **\*Имя(ru)** оставить пустым (если его не задавать, то оно совпадет с пунктом меню **имя**). В окне **Команда** укажите путь к вашему скрипту (для экономии времени можно воспользоваться кнопкой обзора – ...). Нажмите **ОК** и появится ваша кнопка.

Для того чтобы скрипт запускался в консольном режиме – нужно поставить галочку в окошке **Запускать в терминале**.

При необходимости можно изменить рисунок на кнопке. Для этого – нажать на кнопку с рисунком и выбрать понравившееся вам изображение. **ОК** – кнопка готова!

Создайте кнопку на рабочем столе и свяжите ее с помощью скрипта с программой Dr.Web. Запустите программу Dr.Web на выполнение с помощью созданной вами кнопки. Обратите внимание, какая вирусная база у Вас является последней и общее количество сигнатур вирусов в базе – параметр `total virus records` (см. рис. 6.8, на котором видно, что последней вирусной базой является `drw50031`, а общее количество сигнатур вирусов равно `577022`).

### **ЗАДАНИЕ 7. Обновление антивирусных баз ПЭВМ с магнитных носителей**

Как и любой антивирусный пакет, программа Dr.Web нуждается в регулярном обновлении базы данных известных вирусов. Задача эта решается следующим образом: вирусная база состоит из нескольких файлов вида `*.vdb`, представляющих собой отдельные ее части. При появлении новых вирусов выпускаются небольшие (размером в один или несколько Кб) файлы, которые содержат фрагменты базы, описывающие эти вирусы. Эти фрагменты (дополнения вирусной базы) оперативно доступны по адресу

<http://www.antivir.ru/drweb/free>

Дополнения представляют собой единые для всех поддерживаемых платформ файлы вида:

`drwtoday.vdb` (ежедневные обновления);

`drwXXXXX.vdb` (регулярные обновления, появляющиеся обычно еженедельно).

Для того чтобы подключить дополнение к основной вирусной базе, соответствующий файл должен быть помещен в каталог программы Dr.Web (по умолчанию – в `/var/drweb/bases`) или иной каталог, определенный в конфигурационном файле, по умолчанию он размещается в каталоге `/etc/drweb/drweb32.ini`.

Осуществите обновление вирусных баз из каталога ***updates***, находящегося на дистрибутивном диске с программой Dr.Web. Для этого извлеките файлы вирусных баз из архивов с помощью любой программы для работы с архивами (например: `mc`, `tar`, `gzip`, `arc` и т.д.) в папку `/var/drweb/bases`.

С помощью созданной вами кнопки еще раз запустите программу Dr.Web на выполнение. Обратите внимание на то (рис.12), какая вирусная база

теперь является последней (drw500ac) и каково общее количество сигнатур вирусов в базе (total virus records = 3505423).

Будьте готовы осуществить обновление вирусных баз с машинного носителя преподавателя и продемонстрировать работу созданной вами кнопки.

```
[root@VSV-n drweb]# ./drweb -path=/tmp
Dr.Web (R) Scanner for Linux v4.44.0 (4.44.0.0801230)
Copyright (c) Igor Daniloff, 1992-2007
Doctor Web, Ltd., Moscow, Russia
Support service: http://support.drweb.com
To purchase: http://buy.drweb.com
Report dated 2012-10-29, 02:19:45
Command line: -path=/tmp
Shell version: 4.44.0.10060 <API:2.2>
Engine version: 5.0.0.12182 <API:2.2>
Loading /var/drweb/bases/drwtoday.vdb - Ok, virus records: 5605
Loading /var/drweb/bases/drwdaily.vdb - Ok, virus records: 586
Loading /var/drweb/bases/drw500ac.vdb - Ok, virus records: 14727
Loading /var/drweb/bases/drw500ab.vdb - Ok, virus records: 19485
Loading /var/drweb/bases/drw500aa.vdb - Ok, virus records: 22591
Loading /var/drweb/bases/drw500a9.vdb - Ok, virus records: 20551
Total virus records: 3505423
Key file: /opt/drweb/drweb32.key
License key number: 0014065672
License key activates: 2010-03-17
License key expires: 2013-12-31
```

Рис. 12. Окно запуска сканера Dr.Web после обновления вирусных баз

## 5.Отчетность по работе

По выполнению работы каждый курсант должен представить отчет. Отчет должен содержать:

- название практического занятия;
- текст индивидуального задания;
- цель работы;
- результаты проделанной работы;
- Выводы.

В процессе выполнения индивидуального задания или после завершения его выполнения преподаватель проводит собеседование с каждым курсантом по теме выполненной работы, проверяя также практические навыки, приобретенные в ходе занятия. Отчетный материал предоставляется преподавателю, а результаты защищаются.

## 6.Заключительная часть

Товарищи слушатели, на сегодняшнем занятии вы практически отработали вопросы с установкой и обновлением антивирусных баз антивирусного комплекса DrWeb.

На занятии активно и правильно выполняли задания слушатели:\_\_\_им выставлены оценки. На следующем занятии вы перейдете к изучению темы 3 «Особенности построения современного математического обеспечения ЭВМ»

## **МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

Во вступительной части преподавателю объявить тему занятия, его цели, учебные вопросы, порядок его проведения, отметить практическую значимость для пользователя ПК знание антивирусной защиты, используемую литературу.

Проверку готовности слушателей к занятию осуществить проверкой наличия у них рабочих тетрадей, а также постановкой контрольных вопросов по знанию материала предыдущего группового занятия.

Отработку учебных вопросов осуществлять путем выполнения заданий, выдаваемых всей группе.

При отработке первого вопроса основное внимание обратить на приобретение слушателями первоначальных практических навыков в работе с антивирусным комплексом DrWeb, знание обучающимися основных команд для запуска антивирусной проверки. Показать на конкретных примерах.

При отработке второго вопроса прививать практические навыки в самостоятельной работе по обновлению антивирусных баз ПЭВМ с магнитных носителей. Обратить внимание на то, что именно знание основ антивирусной защиты позволит грамотно выполнять свои обязанности в части работы с ПЭВМ.

В заключительной части занятия оценить работу учебной группы в целом, подвести итоги занятия, выставить оценки слушателям, ответить на возникшие вопросы. Сформулировать задание на самоподготовку и объявить тему следующего занятия.

### **7. Задание и методические указания слушателям на самостоятельную подготовку**

1. Изучить Руководство администратора Dr.Web для интернет-шлюзов UNIX (ОС MSVC 3.0).

## **IV. ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА**

1. Руководство администратора Dr.Web для интернет-шлюзов UNIX (ОС MSVC 3.0).
2. РМ «DrWeb для почтовых серверов. Руководство администратора»

Доцент 27 кафедры  
к.т.н.  
подполковник

С. Краснов

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.