

Для служебного пользования


Экз. № \_\_\_\_

УТВЕРЖДАЮ

Врио начальника 8 Управления Генерального штаба  
Вооруженных Сил Российской Федерации  
полковник



А.Колованов

 » марта 2018 г.

**ТИПОВАЯ ИНСТРУКЦИЯ**  
**по настройке комплекса средств антивирусной защиты**  
**информации «Dr.Web Enterprise Security Suite» версии 10.00.1**

Москва, 2018 год

В редакции от 15.05.18

## Содержание

Общие сведения .....	3
1. Установка и настройка сервера централизованной защиты .....	4
2. Порядок обновления баз вирусных сигнатур .....	8
2.1. Обновление БВС в репозитории сервера централизованной защиты .....	8
2.1.1. Через браузер на АРМ офицера по ОБИ .....	8
2.1.2. Через браузер на сервере централизованной защиты .....	11
2.2. Обновление БВС на рабочих станциях .....	12
2.3. Обновление БВС на автономных рабочих станциях .....	13
2.4. Проверка актуальности БВС .....	14
2.4.1. На рабочей станции, подключенной к серверу централизованной защиты .....	14
2.4.2. На автономной рабочей станции .....	14
3. Настройка правил фильтрации межсетевых экранов для обеспечения функционирования антивирусной сети .....	16
4. Создание связи между серверами централизованной защиты .....	17
4.1. Создание связи с сервером централизованной защиты вышестоящей воинской части .....	17
4.2. Создание связи с сервером централизованной защиты подчиненной воинской части .....	19
5. Установка и настройка «Dr.Web для Linux» .....	21
5.1. Сетевая установка .....	21
5.2. Локальная установка .....	23
5.2.1. С использованием скриптов .....	23
5.2.2. С использованием скриптов без подключения к серверу централизованной защиты .....	24
5.2.3. Вручную .....	25
6. Установка и настройка «Агент Dr.Web для Windows» .....	30
7. Журнал подключения и сканирования usb-носителей .....	33
8. Действия при возникновении ошибок .....	34
9. Проверка правильности настроек .....	35
9.1. Сервер централизованной защиты .....	35
9.2. «Dr.Web для Linux» .....	37
Приложение 1 .....	39
Приложение 2 .....	40

## Общие сведения

Настоящая типовая инструкция по настройке комплекса средств антивирусной защиты информации (далее – САВЗ) «Dr.Web Enterprise Security Suite» версии 10.00.1 разработана на основании пункта 23 «Инструкции по организации антивирусной защиты в Вооруженных Силах Российской Федерации», утвержденной приказом Министра обороны Российской Федерации 2014 года № 089, в целях повышения эффективности использования САВЗ, а также принятия эффективных мер по локализации распространения и недопущения негативного воздействия вредоносного программного обеспечения (далее – ВПО) на защищаемые информационные ресурсы с учетом производительности средств вычислительной техники (далее – СВТ).

Типовая инструкция предназначена для использования органами обеспечения безопасности информации (ответственными за защиту информации) воинских частей и организаций Минобороны России при выполнении мероприятий по антивирусной защите информации на объектах информатизации.

Действие настоящей типовой инструкции распространяется на СВТ, не входящие в состав автоматизированных систем военного назначения и функционирующие под управлением операционных систем (далее – ОС) Astra Linux Special Edition 1.5 (далее – Astra Linux), а также операционных систем семейства Windows.

Комплекс САВЗ «Dr.Web Enterprise Security Suite» является сетевой версией САВЗ и предназначен для организации и обеспечения антивирусной защиты информации в рамках как отдельной локально-вычислительной сети (далее – ЛВС), так и в масштабах территориально-распределенной сети передачи данных.

В настоящей Инструкции рассматриваются следующие составные части (модули) комплекса САВЗ «Dr.Web Enterprise Security Suite»:

- сервер централизованной защиты Dr.Web Enterprise Security Suite (далее – сервер централизованной защиты), функционирующий под управлением операционной системы Astra Linux;

- агент Dr.Web для Windows из состава дистрибутива «Dr.Web Enterprise Security Suite» (далее – «агент Dr.Web для Windows»);

- «Антивирус Dr.Web для рабочих станций Linux» (далее – «Dr.Web для Linux»).

Сервер централизованной защиты включает в себя непосредственно сам сервер, встроенную базу данных (драйвера для подключения баз данных сторонних производителей) и центр управления, и предназначен для выполнения функций централизованного администрирования САВЗ, а также мониторинга состояния антивирусной защиты информации на защищаемых СВТ.

«Агент Dr.Web для Windows» и «Dr.Web для Linux» предназначены непосредственно для обеспечения защиты СВТ от ВПО, а также выполняют функции по взаимодействию с сервером централизованной защиты.

«Агент Dr.Web для Windows» представлен в виде исполняемого файла `drweb-esuite-agent-full-10.00.1-201703021-windows.exe`, «Dr.Web для Linux» – в виде файла `drweb-workstations_11.0.2-1703021323+mo-linux_amd64.run`. Дистрибутивы могут функционировать как в автономном режиме, так и в режиме централизованной защиты.

В «Dr.Web Enterprise Security Suite» версии 10.00.1 уникальный идентификатор сервера хранится в соответствующем конфигурационном файле, а не в лицензионном ключевом файле `enterprise.key`, поэтому для корректного функционирования сервера и подключенных к нему станций **необходим только ключ для станций – `agent.key`.**

**Для автоматизации процесса развертывания и настройки сервера централизованной защиты, а также удаленной сетевой установки «Dr.Web для Linux» применяются скрипты, подготовленные 3 центром войсковой части 31659.**

### **1. Установка и настройка сервера централизованной защиты**

Установка сервера централизованной защиты и первоначальная настройка осуществляется с помощью архива **`DRW_ESS_10.00.1_install_script.tar.gz`.**

**Перед началом установки сервера централизованной защиты необходимо:**

1. Зайти в ОС под учетной записью суперпользователя (root).
2. Скопировать архив `DRW_ESS_10.00.1_install_script.tar.gz` и файл с контрольной суммой (`DRW_ESS_10.00.1_install_script.tar.gz.md5`) на рабочий стол (каталог `/root/Desktop/`) на СБТ, которое планируется использовать в качестве сервера централизованной защиты (в качестве такого СБТ рекомендуется применять серверное оборудование).

3. Перейти в директорию рабочего стола и проверить контрольную сумму установочного файла, выполнив команды:

```
cd /root/Desktop
md5sum DRW_ESS_10.00.1_install_script.tar.gz
cat DRW_ESS_10.00.1_install_script.tar.gz.md5
```

Выводы команд `md5sum` и `cat` должны совпадать, в противном случае целостность установочного файла нарушена и необходимо повторно скопировать указанные выше файлы.

*Примечание: ключевой комплект `agent.key` уже включен в состав архива `DRW_ESS_10.00.1_install_script.tar.gz`.*

**Для установки сервера централизованной защиты необходимо:**

1. Запустить консоль «Терминал Fly» (Пуск → Утилиты → Терминал Fly).

2. В консоли сменить рабочий каталог, выполнив команду:

```
cd /root/Desktop
```

3. Распаковать архив `DRW_ESS_10.00.1_install_script.tar.gz`, выполнив команду:

```
tar -xzf DRW_ESS_10.00.1_install_script.tar.gz
```

4. Перейти в папку `drw_ess_install_script`, выполнив команду:

```
cd drw_ess_install_script
```

5. Произвести установку и первоначальную настройку, выполнив команды:


```
chmod +x drw_ess_setup.sh  
./drw_ess_setup.sh
```

6. Ввести необходимые данные (название сервера и IP-адрес) по запросу установочного скрипта.

В процессе выполнения файла-скрипта осуществляется:

*проверка актуальности ключевого комплекта agent.key;*

*установка сервера централизованной защиты с расширением браузера;*

*замена шаблона repository.js для возможности выбора импортируемого архива с актуальными обновления БВС (значок «Лупы» );*

*установка файла лицензионного ключа и его распространение на группы администрирования;*

*настройка автоматического подтверждения подключаемых к серверу централизованной защиты рабочих станций;*

*включение протоколов сервера централизованной защиты для разрешения взаимодействия между связанными серверами, а также для подключения утилиты удаленной диагностики;*

*настройка расписания задач сервера централизованной защиты и задач по проведению автоматических проверок на наличие ВПО;*

*создание учетной записи на сервере централизованной защиты для контроля настроек и функционирования антивирусной сети администратором аудита (с правами «только для чтения»).*

*установка «Dr.Web для Linux» на СБТ, где происходит установка сервера централизованной защиты.*

По завершению установки на экран будет выведена строка:

```
[OK] Dr.Web 11 for Linux Workstations was successfully  
installed and connected to DRW ESS 10.00.1 server.
```

7. В случае возникновения ошибок перейти к [разделу 8](#).

8. Добавить учетную запись администратора с правами «только для чтения» с именем **auditor** для вышестоящего штаба для контроля состояния антивирусной защиты подчиненных воинских частей. Для этого необходимо выполнить следующую команду в терминале на сервере централизованной защиты:

```
curl -s --user admin:root  
"http://localhost:9080/api/admins/add.ds?login=auditor&password=  
пароль&readonly=yes",
```

где admin:root – логин и пароль учетной записи администратора центра управления сервера централизованной защиты по умолчанию;

login=auditor – имя учетной записи вышестоящего штаба;

password=пароль – указать вместо строки «пароль» пароль учетной записи вышестоящего штаба.

После выполнения команды будет выведено сообщение, в параметре status которого должно быть значение true, что означает успешное создание учетной записи:

```
<?xml version="1.0" encoding="UTF-8"?> <drweb-es-api  
api_version="4.0.3" timestamp="1521631976" server="localhost"  
srv_version="10.00.1.201702110" status="true"> <administrator  
id="78bd53bc-8fb5-4e55-971e-b7fc0a1b7c87" /> </drweb-es-api>
```

9. Запустить веб-браузер Mozilla Firefox: Пуск → Сеть → Mozilla Firefox.

10. Ввести в адресную строку браузера IP-адрес сервера централизованной защиты, знак двоеточия «:», номер порта (по умолчанию «9080») и нажать клавишу «Enter», например 192.168.77.128:9080.

11. На загрузившейся странице веб-браузера ввести аутентификационные данные для доступа к центру управления сервера централизованной защиты (значения по умолчанию: логин «admin», пароль «root») и нажать кнопку «ОК».

12. Перейти в меню Администрирование > Конфигурация > Администраторы. Раскрыть группу «Administrators». Выбрать пользователя admin. Нажать кнопку «Изменить пароль» (🔑). Дважды ввести новый пароль и нажать кнопку «Сохранить» (рисунок 1).

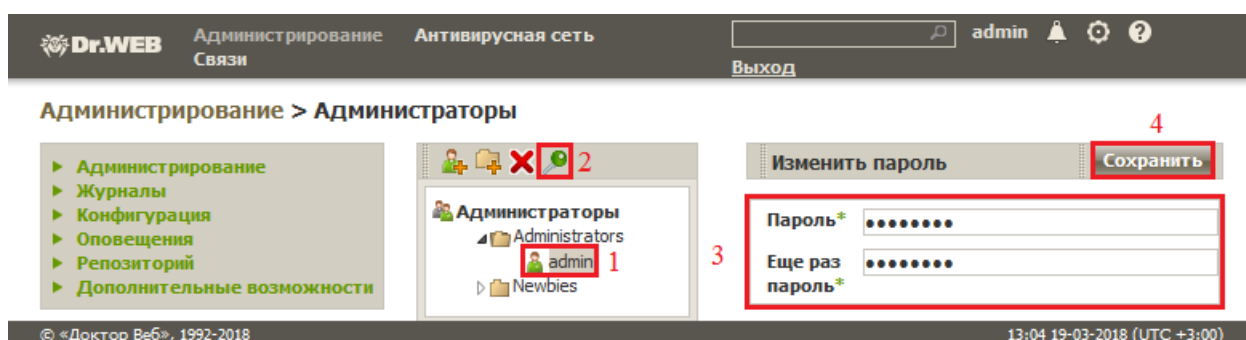


Рисунок 1. Изменение пароля учетной записи администратора

13. При необходимости можно добавить дополнительную учетную запись с правами администратора. Для этого в меню Администрирование > Конфигурация > Администраторы нажать кнопку «Создать учетную запись». Ввести «Регистрационное имя» добавляемого пользователя. Выбрать «Тип аутентификации» – Внутренняя. Дважды указать пароль. Выбрать «Язык интерфейса» – Русский. Проверить, чтобы в Разделе «Группы» стояла галочка напротив группы «Administrators». Нажать кнопку «Сохранить» (рисунок 2).

Dr.WEB    Администрирование    Антивирусная сеть    admin    ?    Выход

Администрирование > Администраторы

- Администрирование
- Журналы
- Конфигурация
- Оповещения
- Репозиторий
- Дополнительные возможности

1

Администраторы

- Administrators
- Newbies

Новая учетная запись администратора

Сохранить 8

Общие

Регистрационное имя\* user\_name 2

Тип аутентификации

☒ Внутренняя 3

☐ Внешняя

Пароль\* ..... 4

Еще раз пароль\* ..... 5

Имя

Отчество

Фамилия

Язык интерфейса Русский 6

Формат даты DD-MM-YYYY HH:MM:SS

Описание

Группы

☒ Administrators 7

☐ Newbies

© «Доктор Веб», 1992-2018    13:09 19-03-2018 (UTC +3:00)

Рисунок 2. Создание дополнительной учетной записи администратора

## 2. Порядок обновления баз вирусных сигнатур

Обновление баз вирусных сигнатур (далее – БВС), выполняется в два этапа:

1. Обновление БВС в репозитории сервера централизованной защиты;
2. Обновление БВС на станциях, подключенных к серверу централизованной защиты.

Далее приводится подробное описание того, как правильно выполнить обновление БВС и убедиться в отсутствии ошибок.

### 2.1. Обновление БВС в репозитории сервера централизованной защиты

#### 2.1.1. Через браузер на АРМ офицера по ОБИ



1. Скопировать архив, содержащий обновления БВС, и файл с контрольной суммой на АРМ офицера по ОБИ.

2. Перейти в директорию рабочего стола и проверить контрольную сумму загруженного архива, выполнив команды:

```
cd /root/Desktop  
md5sum DRW_ESS11_YYYYMMDD1.zip  
cat DRW_ESS11_YYYYMMDD.md5
```

Выводы команд `md5sum` и `cat` должны совпадать, в противном случае целостность архива с обновлениями нарушена и необходимо повторно скопировать указанные выше файлы.

3. Запустить веб-браузер Mozilla Firefox и подключиться к центру управления.

4. Перейти в раздел «Администрирование» → «Содержимое репозитория», нажать кнопку «Импортировать архив с файлами репозитория» () , установить настройки импорта согласно рисунку и нажать кнопку «Лупа» () для выбора файла обновлений. В открывшемся окне выбрать необходимый архив и нажать кнопку «Открыть», после чего нажать кнопку «Импортировать» (рисунок 3).

---

<sup>1</sup> YYYYMMDD – соответственно, год, месяц и день



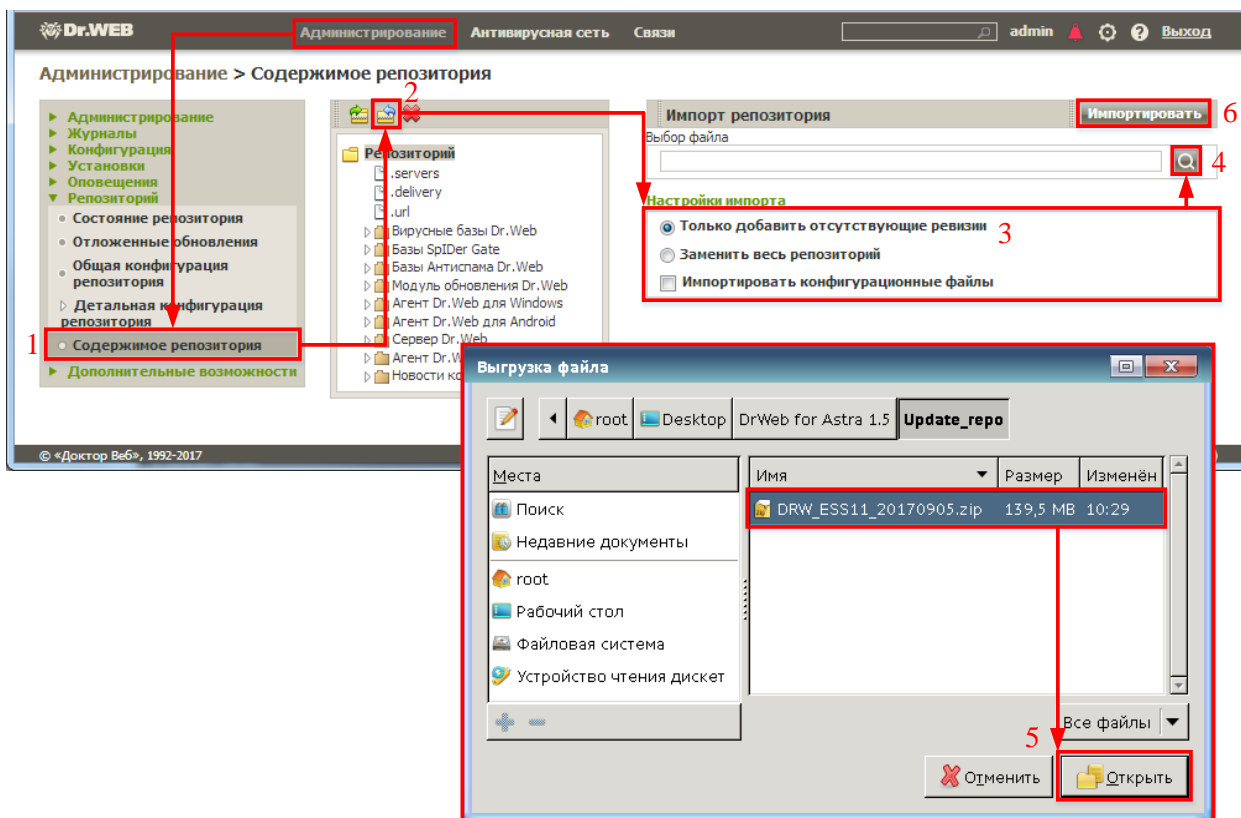


Рисунок 3. Обновление репозитория сервера централизованной защиты

После нажатия кнопки «Импортировать» в титуле открытой вкладки появится индикатор ожидания, а слева внизу появится сообщение «Отправка запроса на ...», что свидетельствует о начале процесса загрузки обновлений БВС на сервер (рисунок 4).

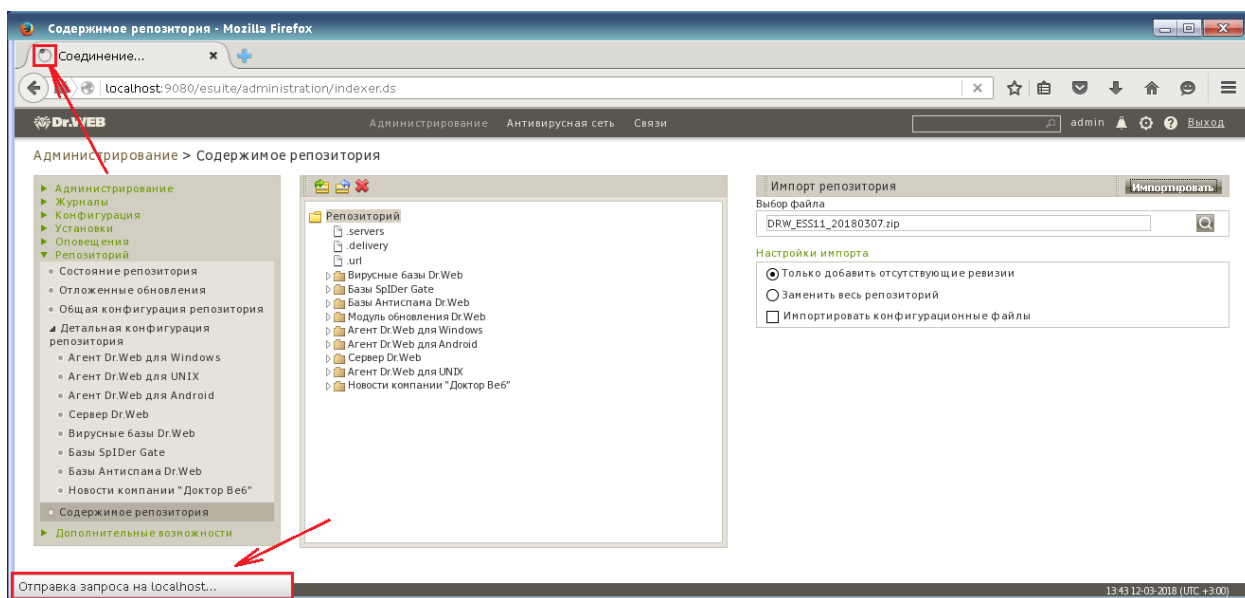


Рисунок 4. Индикаторы работы процесса обновления репозитория сервера централизованной защиты

После окончания операции импорта в титуле открытой вкладки появится значок Dr.Web, а сообщение слева внизу пропадет (рисунок 5).

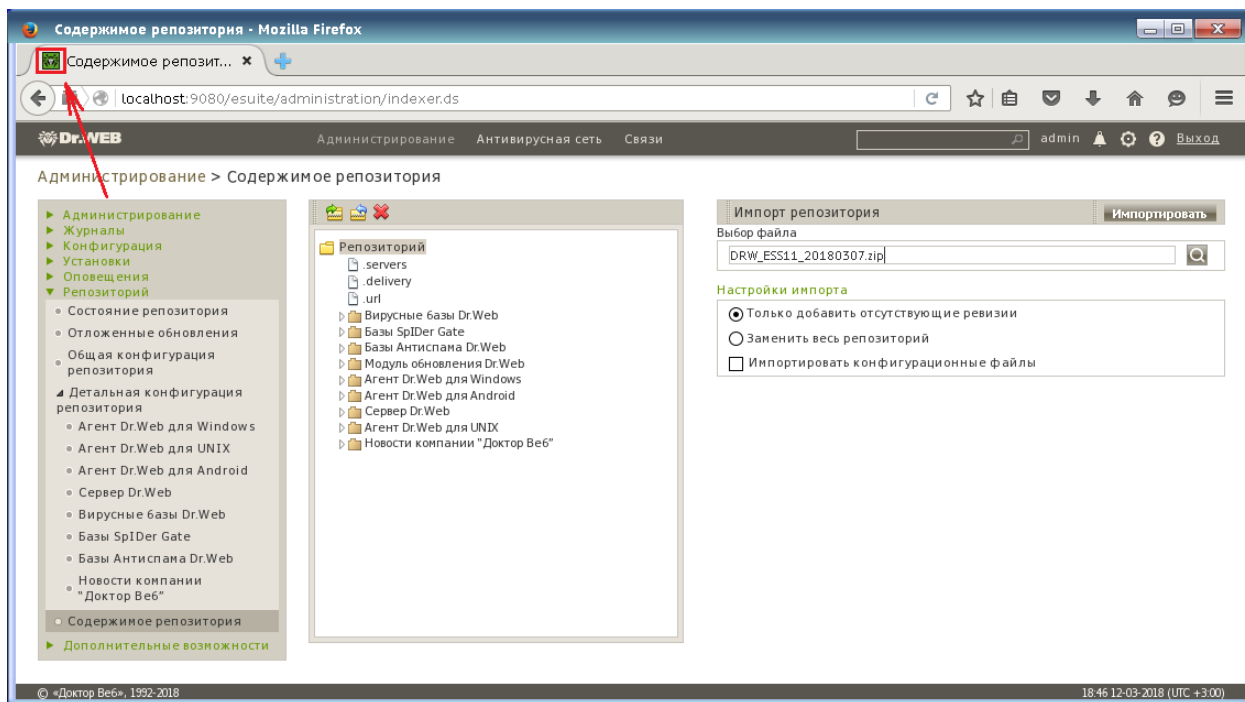


Рисунок 5. Индикаторы завершения процедуры обновления репозитория сервера централизованной защиты

5. Проверить состояние репозитория после обновления. Для этого необходимо перейти в «Администрирование → Состояние репозитория» и проверить дату в столбце «Текущая ревизия» в строке «Вирусные базы Dr.Web», которая должна соответствовать дате в имени импортируемого архива (рисунок 6).

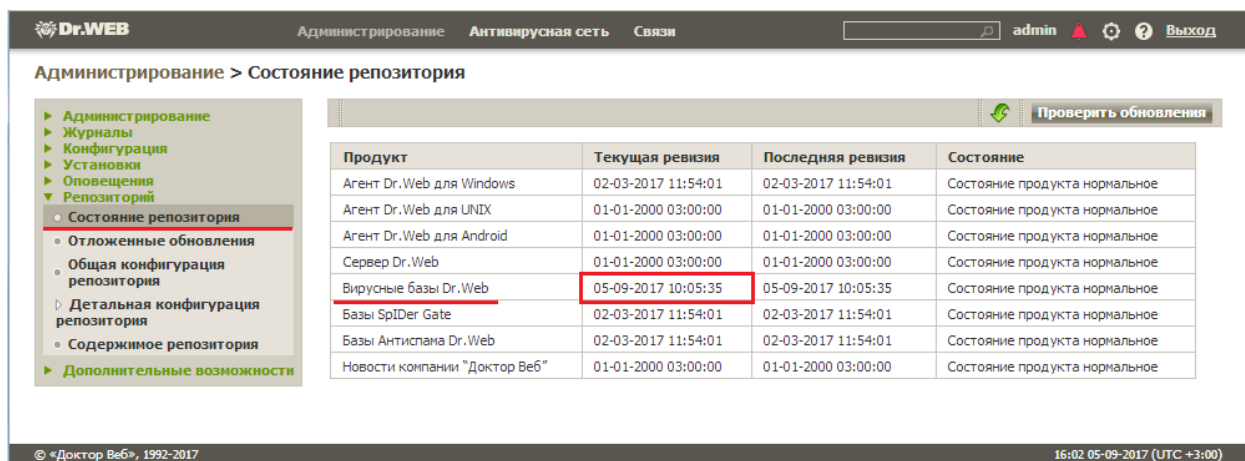


Рисунок 6. Проверка успешного завершения обновления репозитория сервера централизованной защиты

### 2.1.2. Через браузер на сервере централизованной защиты

1. Скопировать архив, содержащий обновления БВС, и файл с контрольной суммой на рабочий стол (каталог /root/Desktop/) сервера централизованной защиты.

*Примечание: для копирования можно использовать утилиты scp на Astra Linux или WinSCP на Windows.*

2. Подключиться к серверу централизованной защиты, используя протокол ssh.

```
ssh root@<IP-адрес-сервера-централизованной-защиты>
```

или

```
ssh <учетная-запись-пользователя-с-правами-на-выполнение-команд-супер-пользователя>@<IP-адрес-сервера-централизованной-защиты>
```

3. Перейти в директорию рабочего стола и проверить контрольную сумму загруженного архива, выполнив команды:

```
cd /root/Desktop
md5sum DRW_ESS11_[дата выхода обновлений].zip
cat DRW_ESS11_[дата выхода обновлений].md5
```

Выводы команд md5sum и cat должны совпадать, в противном случае целостность архива с обновлениями нарушена и необходимо повторно скопировать указанные выше файлы.

4. Подключиться к серверу централизованной защиты через утилиту удаленного рабочего стола (подробнее в [Приложении 1](#)).

5. Выполнить пункты 3, 4, 5 [раздела 2.1.1](#).

## 2.2. Обновление БВС на рабочих станциях

Сервер централизованной защиты оповещает о появлении обновлений БВС в репозитории:

1. Подключенные и включенные станции;
2. При подключении станции к серверу (сервер сообщает станции, что есть в репозитории сервера).

Таким образом, обновление БВС на рабочих станциях, подключенных к серверу централизованной защиты, должно происходить **автоматически**, если в разделе «Состояние» для группы Everyone на этих рабочих станциях отсутствуют сообщения об ошибках.

Для проверки состояния рабочих станций для группы Everyone, необходимо:

1. Запустить веб-браузер Mozilla Firefox и подключиться к центру управления.
2. Перейти по ссылке «Антивирусная сеть», выделить группу «Everyone» (убедиться, что в разделе «Выбранные объекты» отображается папка «Everyone») и в разделе «Статистика» нажать на строку «Состояние». На открывшейся странице должна появиться таблица с информацией о состоянии каждой подключенной станции. В данной таблице не должно быть сообщений об ошибках в вирусных базах с «Серьезностью» выше «Средней» (рисунок 7).

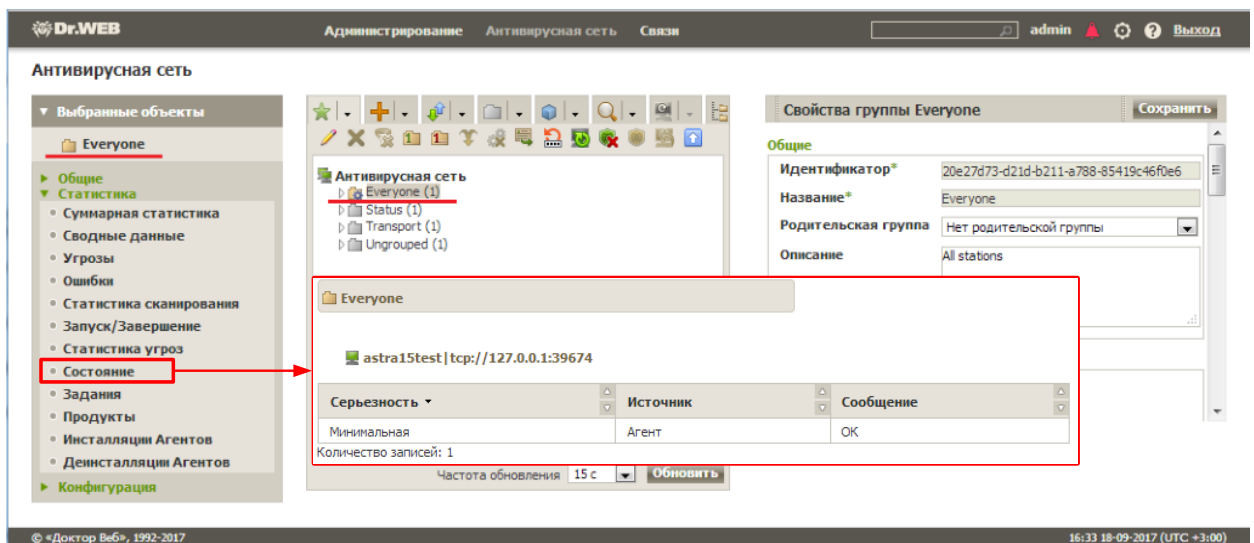


Рисунок 7. Проверка состояния станций, подключенных к серверу централизованной защиты

### 2.3. Обновление БВС на автономных рабочих станциях

Для обновления БВС на автономной рабочей станции необходимо:

1. Войти в систему под учетной записью суперпользователя (root).  
2. Скопировать архив DRW\_Linux11\_YYYYMMDD<sup>2</sup>.rar и файл с контрольной суммой (DRW\_Linux11\_YYYYMMDD.rar.md5) на рабочий стол (каталог /root/Desktop/).

3. Перейти в директорию рабочего стола и проверить контрольную сумму загруженного архива, выполнив команды:

```
cd /root/Desktop  
md5sum DRW_Linux11_YYYYMMDD.rar  
cat DRW_Linux11_YYYYMMDD.md5
```

Выводы команд md5sum и cat должны совпадать, в противном случае целостность архива с обновлениями нарушена и необходимо повторно скопировать указанные выше файлы.

4. Распаковать rar-архив с помощью команды:

```
unrar x -inul DRW_Linux11_YYYYMMDD.rar
```

5. Скопировать содержимое каталога bases, извлеченного из архива в предыдущем пункте, в каталог /var/opt/drweb.com/bases/

```
cp bases/* /var/opt/drweb.com/bases/
```

6. Перезапустить демона drweb-configd, чтобы антивирус перечитал БВС:

```
service drweb-configd restart
```

7. После успешной перезагрузки демона drweb-configd подождать 10 секунд и выполнить команду drweb-ctl baseinfo для проверки, что БВС успешно загружены САВЗ. Если при выполнении команды drweb-ctl baseinfo будет выведено:

```
Core engine: 7.00.27.02270
```

```
Virus bases are not loaded
```

```
Last successful update: unknown
```

Это означает, что БВС еще не загружены демоном drweb-configd и нужно подождать несколько секунд и повторно выполнить команду drweb-ctl baseinfo.

8. Проверить, чтобы в строке Virus base timestamp отображалась актуальная дата (не старше недели), соответствующая временной метке (YYYYMMDD) в названии загруженного архива обновлений. В случае несоответствия отображаемой даты в строке Virus base timestamp с временной меткой загруженного архива обновлений необходимо доложить об этом в вышестоящую воинскую часть.

9. На восклицательный знак на желтом фоне на значке «Dr.Web для Linux» в правом нижнем углу внимание не обращать не стоит, если в главном окне графического интерфейса «Dr.Web для Linux» отображается предупреждение «Требуется обновление» (подробнее в [разделе 2.4.2](#)). В случае, если восклицательный знак на желтом фоне отображается по другой причине (не из-за обновлений БВС), необходимо выявить причину его появления и восстановить работу САВЗ.

---

<sup>2</sup> YYYYMMDD – соответственно, год, месяц и день

## 2.4. Проверка актуальности БВС

В данном разделе представлены методы проверки актуальности БВС на автономных рабочих станциях и на рабочих станциях, подключенных к серверу централизованной защиты.

### 2.4.1. На рабочей станции, подключенной к серверу централизованной защиты

Для проверки актуальности БВС на рабочей станции, подключенной к серверу централизованной защиты, необходимо на АРМ офицера по ОБИ:

1. Запустить веб-браузер Mozilla Firefox и подключиться к центру управления (<http://IP-адрес-сервера-централизованной-защиты:9080>).

2. Перейти по ссылке «Антивирусная сеть», выделить станцию для проверки даты обновления БВС (убедиться, что в разделе «Выбранные объекты» отображается название выбранной станции) и в разделе «Статистика» нажать на строку «Вирусные базы». На открывшейся странице должна появиться таблица с информацией о дате выпуска БВС. В данной таблице необходимо нажать на стрелочку «Вниз» в столбце «Выпущена» для сортировки значений по убыванию (рисунок 8). Дата выпуска файлов с названиями dwmtoday.vdb, dwntoday.vdb, dwrtoday.vdb, drwtoday.vdb должна соответствовать дате текущей ревизии продукта «Вирусные базы Dr.Web» на странице «Состояние репозитория» сервера централизованной защиты (рисунок 6).

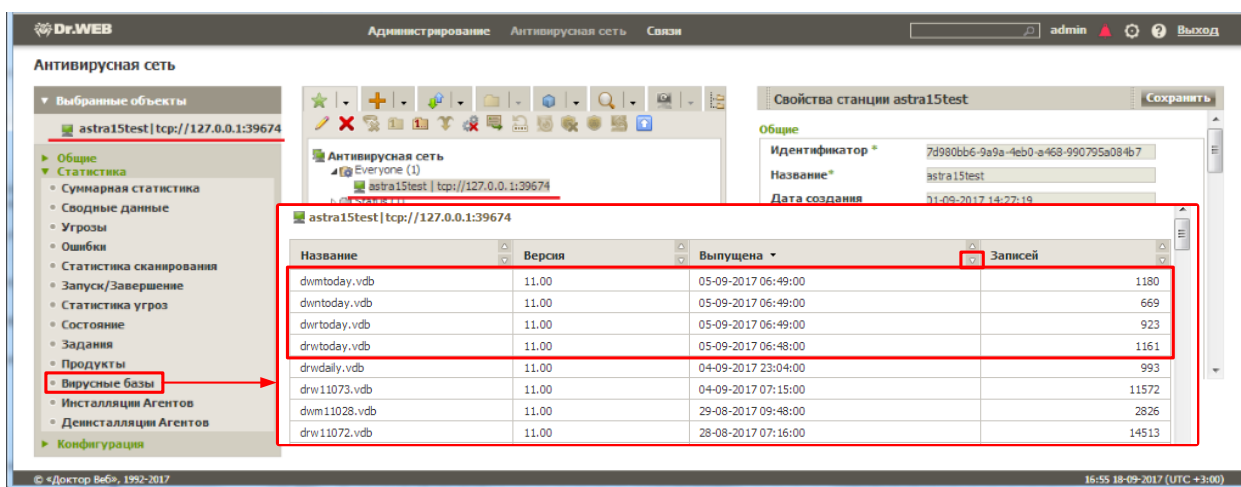
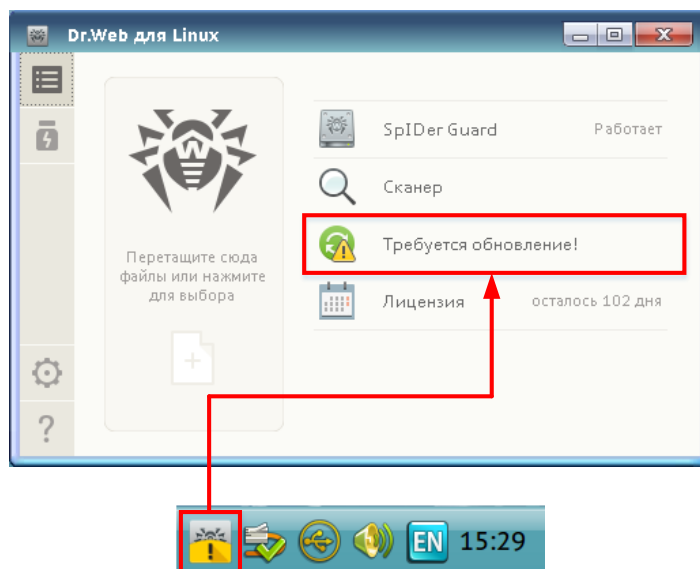


Рисунок 8. Проверка даты выпуска обновлений БВС для конкретной станции, подключенной к серверу централизованной защиты

### 2.4.2. На автономной рабочей станции

Сразу после установки сертифицированной версии «Dr.Web для Linux» версии 11.0.2 (дистрибутив drweb-workstations\_11.0.2-1703021323+mo-linux\_amd64.run) на значке в правом нижнем углу, а также в главном окне графического интерфейса «Dr.Web для Linux» (рисунок 9), будет отображаться восклицательный знак на желтом фоне с надписью «Требуется обновление».





*Рисунок 9. Недостоверный индикатор необходимости обновления БВС  
«Dr.Web для Linux»*

По данным технической поддержки ООО «Доктор Веб», в данной версии этот восклицательный знак на желтом фоне можно убрать только если обновить БВС с серверов обновлений Dr.Web в Интернете, либо в режиме централизованной защиты с сервера централизованной защиты, что на автономных АРМ выполнить не представляется возможным. Подобное поведение будет исправлено в следующей сертифицированной версии (когда при обновлении БВС на автономном АРМ в главном окне графического интерфейса «Dr.Web для Linux» и на значке в правом нижнем углу будут отсутствовать восклицательный знак на желтом фоне и сообщение «Требуется обновление»).

Дату выпуска БВС необходимо отслеживать, запуская следующую команду в терминале Fly (для выполнения не требует наличия прав супер пользователя):

```
drweb-ctl baseinfo
```

Вывод команды:

```
Core engine: 7.00.27.02270
```

```
Virus base timestamp: 2018-Mar-21 05:36:27
```

```
Virus base records: 6758234
```

```
Last successful update: unknown
```

В строке Virus base timestamp отображается дата выпуска БВС, которая должна быть актуальной (не старше недели). В строке Virus base records отображается количество вирусных сигнатур в базах.

Вывод команды:

```
Core engine: 7.00.27.02270
```

```
Virus base timestamp: 2018-Mar-21 05:36:27
```

```
Virus base records: 6758234
```

```
Last successful update: unknown
```

Данная команда не требует прав супер пользователя для выполнения.

В строке Virus base timestamp указана дата выпуска БВС, в строке Virus base records указано общее количество вирусных сигнатур в базах. Для поддержания БВС в актуальном состоянии необходимо, чтобы дата в строке Virus base timestamp была также актуальной (не старше недели).

### 3. Настройка правил фильтрации межсетевых экранов для обеспечения функционирования антивирусной сети

Для связи «Dr.Web для Linux» на рабочих станциях с сервером централизованной защиты, а также для межсерверного взаимодействия используются порты, приведенные в таблице 1.

Номера портов	Протоколы	Назначение
2193	TCP	Для связи антивирусных компонентов с сервером централизованной защиты и межсерверных связей и для работы «Сканера сети».
2193	UDP	
9080	HTTP	Для подключения к Центру управления сервером централизованной защиты.
9081	HTTPS	
10101	TCP	Для работы утилиты удаленной диагностики сервера централизованной защиты.
3389	TCP	Для удаленного подключения к серверу централизованной защиты в графическом режиме.

*Таблица 1. Порты, необходимые для работы инфраструктуры Dr.Web Enterprise Security Suite*

В таблице 2 указаны направления, которые должны быть открыты на межсетевых экранах для корректной работы инфраструктуры Dr.Web Enterprise Security Suite.

Направления		Номера портов	Протоколы
FROM	TO		
подсеть рабочих станций	#DRW_ESS_IP <sup>3</sup> #	2193	TCP
подсеть рабочих станций	#DRW_ESS_IP#	2193	UDP
#DRW_ESS_IP#	#DRW_ESS_IP#	2193	TCP
#DRW_ESS_IP#	#DRW_ESS_IP#	2193	UDP
#OBI_IP <sup>4</sup> #	#DRW_ESS_IP#	9080	HTTP
#OBI_IP#	#DRW_ESS_IP#	9081	HTTPS
#OBI_IP#	#DRW_ESS_IP#	10101	TCP
#OBI_IP#	#DRW_ESS_IP#	3389	TCP

*Таблица 2. Направления открытия портов, необходимых для работы инфраструктуры Dr.Web Enterprise Security Suite, на межсетевых экранах*

Более подробная информация об открытии портов в указанных выше направлениях описана в «Методике (контрольный пример) настройки средств защиты информации Министерства обороны Российской Федерации», утвержденной Начальником 8 Управления ГШ ВС РФ мая 2018 г.

<sup>3</sup> IP-адрес сервера централизованной защиты

<sup>4</sup> IP-адрес АРМ офицера по ОБИ



## 4. Создание связи между серверами централизованной защиты

### 4.1. Создание связи с сервером централизованной защиты вышестоящей воинской части

Для подключения сервера централизованной защиты воинской части к серверу централизованной защиты вышестоящей воинской части необходимо:

1. Подключиться к центру управления сервера централизованной защиты воинской части (далее – подчиненной воинской части).

2. Проверить, чтобы в конфигурации сервера Dr.Web (Центр Управления → Администрирование → Конфигурация Сервера Dr.Web) присутствовали следующие настройки:


– вкладка «Общие» → Поле «Название» содержит имя сервера<sup>5</sup>.

– вкладка «Модули» → Протокол Сервера Dr.Web должен быть отмечен.

3. Перейти в раздел «Связи» в главном меню для добавления сервера централизованной защиты вышестоящей воинской части в список взаимодействующих серверов<sup>6</sup>.

4. В открывшемся окне на панели инструментов нажать на кнопку «Создать связь».

5. В окне описания связей между серверами выбрать тип «Главный», а также ввести название сервера централизованной защиты вышестоящей воинской части и пароль.

6. Справа от поля «Ключи соседнего Сервера Dr.Web» нажать на кнопку «Лупа» () и указать файл ключа «drwcsd.pub», относящийся к серверу централизованной защиты **вышестоящей воинской части**.

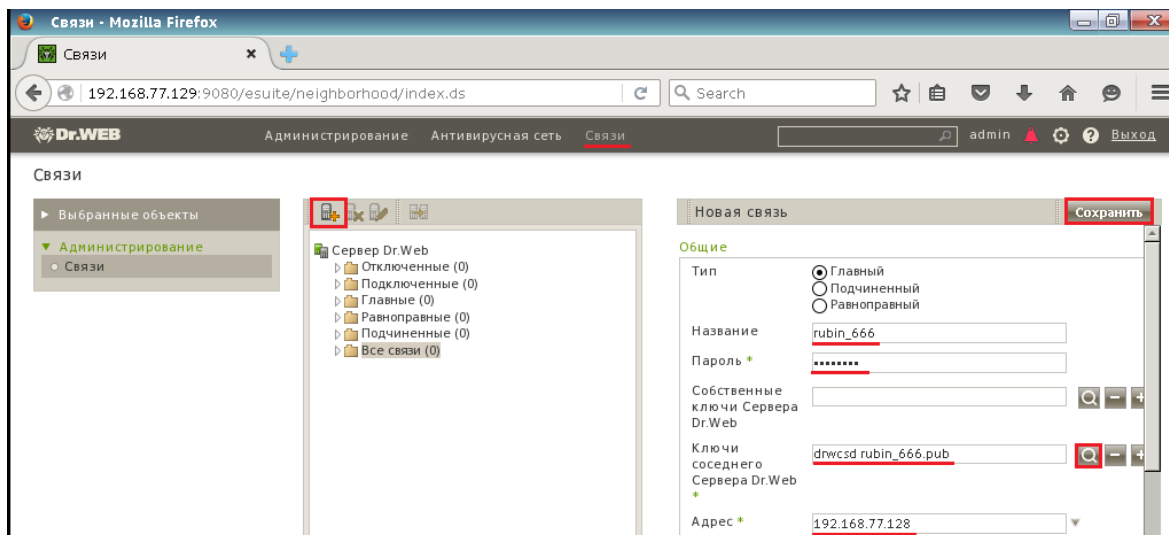
7. В поле «Адрес» ввести IP-адрес сервера централизованной защиты вышестоящей воинской части, остальные поля оставить без изменений.

Нажать кнопку «Сохранить» (рисунок 10).

---

<sup>5</sup> Имя сервера определяется из названия позывного узла связи и условного наименования воинской части. Например, для воинской части 12345, позывной узла связи Зарево, имя сервера Zarevo\_12345

<sup>6</sup> Имя сервера, пароль, файл ключа drwcsd.pub и IP-адрес сервера централизованной защиты вышестоящего штаба доводится до подчиненных служб ЗГТ и подразделений ОБИ вышестоящей службой ЗГТ.

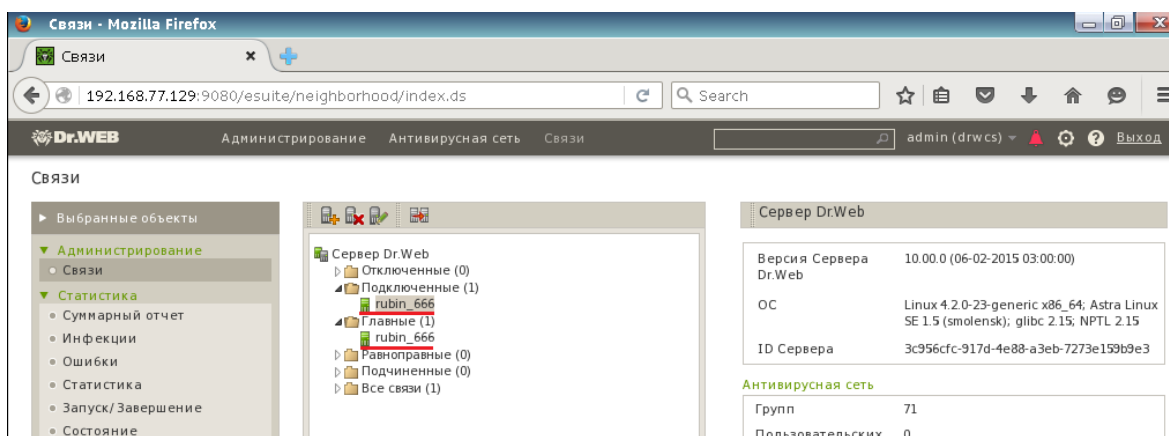


*Рисунок 10. Добавление сервера вышестоящей воинской части на сервере подчиненной воинской части*

В результате иконка сервера централизованной защиты вышестоящей воинской части отобразится в папке Главные и Отключенные.

После установления связи между сервером централизованной защиты подчиненной воинской части и сервером централизованной защиты вышестоящей воинской части иконка сервера централизованной защиты вышестоящей воинской части отобразится в папке «Подключенные» (Рисунок 11).

*Примечание:* для успешного установления связи необходимо, чтобы подобные действия проводились и на сервере централизованной защиты вышестоящей воинской части. Ответственному за работу с сервером централизованной защиты вышестоящей воинской части необходимо создать связь типа «Подчиненный» с использованием ключа «drwcsd.pub», относящегося к серверу централизованной защиты **подчиненной воинской части**.



*Рисунок 11. Отображение подключенного сервера вышестоящей воинской части на сервере подчиненной воинской части*

## 4.2. Создание связи с сервером централизованной защиты подчиненной воинской части

Для подключения сервера централизованной защиты подчиненной воинской части к серверу централизованной защиты воинской части необходимо:

1. Подключиться к центру управления сервера централизованной защиты воинской части (далее – вышестоящей воинской части).

2. Проверить, чтобы в конфигурации сервера Dr.Web (Центр Управления → Администрирование → Конфигурация Сервера Dr.Web) присутствовали следующие настройки:


– вкладка «Общие» → Поле «Название» должно быть уникальное имя сервера.

– вкладка «Модули» → Протокол Сервера Dr.Web должен быть отмечен.

3. Перейти в раздел «Связи» в главном меню для добавления сервера централизованной защиты подчиненной воинской части в список взаимодействующих серверов<sup>7</sup>.

4. В открывшемся окне на панели инструментов нажать на кнопку «Создать связь».

5. В окне описания связей между серверами выбрать тип «Подчиненный», а также ввести название сервера централизованной защиты подчиненной воинской части и пароль.

6. Справа от поля «Ключи соседнего Сервера Dr.Web» нажать на кнопку «Лупа» (  ) и указать файл ключа «drwcsd.pub», относящийся к серверу централизованной защиты **подчиненной воинской части**.

Нажать кнопку «Сохранить» (рисунок 12).

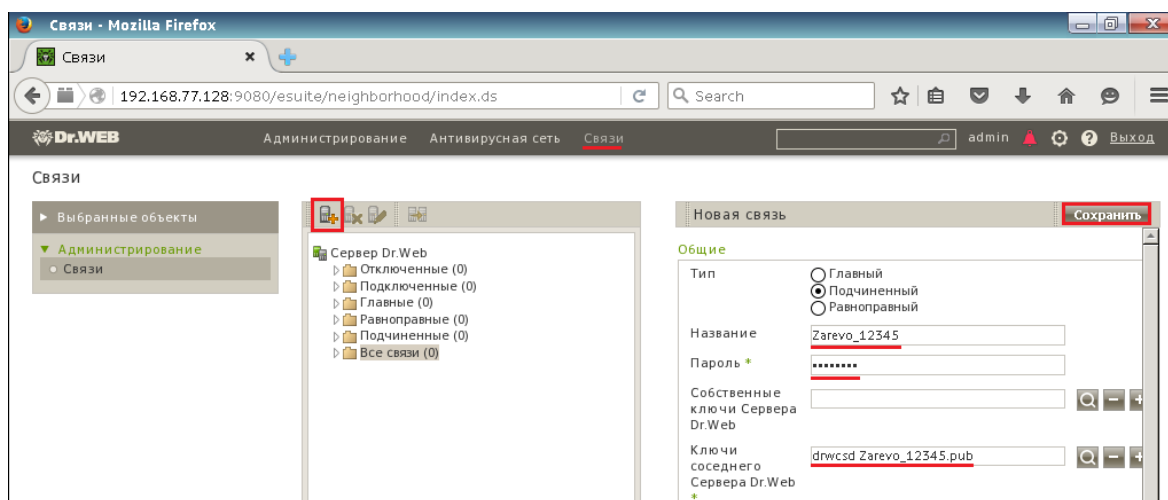


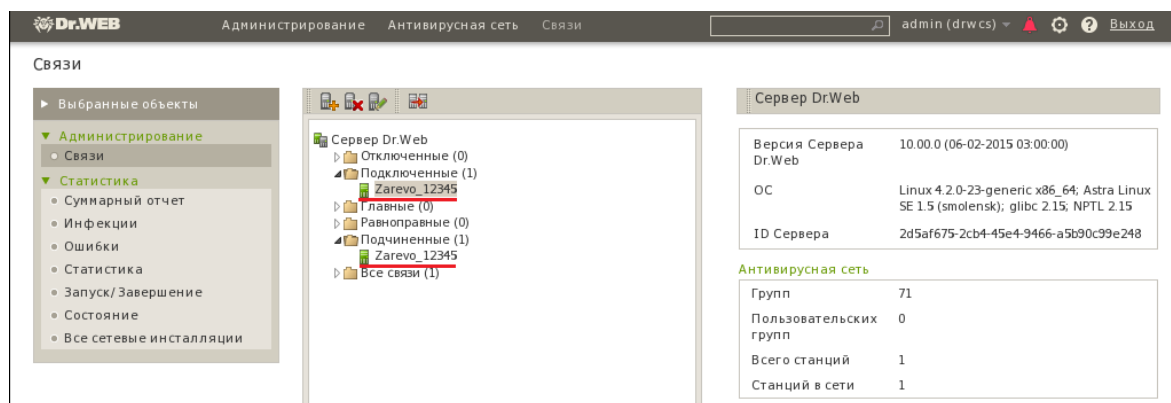
Рисунок 12. Добавление сервера подчиненной воинской части на сервере вышестоящей воинской части

В результате иконка сервера централизованной защиты подчиненной воинской части отобразится в папках Подчиненные и Отключенные.

<sup>7</sup> Имя сервера, пароль, файл ключа drwcsd.pub и IP-адрес сервера централизованной защиты вышестоящего штаба доводится до подчиненных служб ЗГТ и подразделений ОБИ вышестоящей службой ЗГТ.

*Примечание: для успешного установления связи необходимо, чтобы подобные действия проводились и на сервере централизованной защиты подчиненной воинской части. Ответственному за работу с сервером централизованной защиты подчиненной воинской части необходимо создать связь типа «Главный» с использованием ключа «drwcsd.pub», относящегося к серверу централизованной защиты **вышестоящей** воинской части.*

После установления связи между сервером централизованной защиты вышестоящей воинской части и сервером централизованной защиты подчиненной воинской части иконка сервера централизованной защиты подчиненной воинской части отобразится в папке «Подключенные» (рисунок 13).



*Рисунок 13 Отображение подключенного сервера подчиненной воинской части на сервере вышестоящей воинской части*

## 5. Установка и настройка «Dr.Web для Linux»

«Dr.Web для Linux» устанавливается на СБТ под управлением ОС Astra Linux.

Установка «Dr.Web для Linux» возможна двумя способами: локально и по сети. Если конфигурация сети настроена правильно и администратор безопасности информации с АРМ АБИ имеет доступ по протоколу ssh (secure shell) ко всем СБТ ЛВС, то целесообразно производить установку «Dr.Web для Linux» по сети. В противном случае, в том числе при технической неисправности АРМ АБИ, необходимо локально установить «Dr.Web для Linux» на каждом СБТ.

### 5.1. Сетевая установка

**Для установки «Dr.Web для Linux» необходимо:**

1. Зайти на АРМ АБИ в систему под учетной записью суперпользователя (root).

2. Скопировать архив DRW11\_Linux\_Workstations.tar.gz и файл с контрольной суммой (DRW11\_Linux\_Workstations.tar.gz.md5) на рабочий стол (каталог /root/Desktop/).

3. Перейти в директорию рабочего стола и проверить контрольную сумму установочного файла, выполнив команды:

```
cd /root/Desktop
md5sum DRW11_Linux_Workstations.tar.gz
cat DRW11_Linux_Workstations.tar.gz.md5
```

Выводы команд md5sum и cat должны совпадать, в противном случае целостность установочного файла нарушена и необходимо повторно скопировать указанные выше файлы.

4. Запустить консоль «Fly-терминал»:

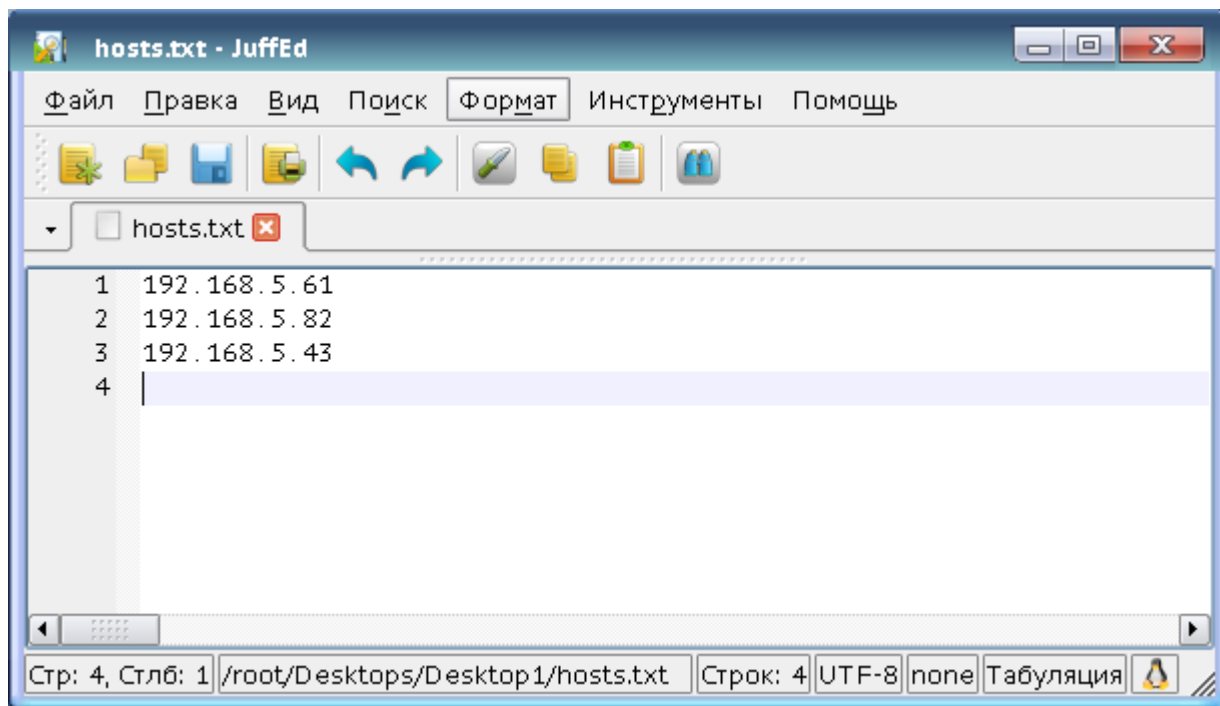
Пуск → Утилиты → Терминал Fly.

5. Перейти в каталог /root/Desktop/ и распаковать архив DRW11\_Linux\_Workstations\_install\_script.tar.gz. Для этого ввести следующие команды:

```
cd /root/Desktop/
tar -xzvf DRW11_Linux_Workstations_install_script.tar.gz
```

6. Перейти в каталог /root/Desktop/drw\_install\_script и создать в нём текстовый файл hosts.txt. Открыть его с помощью текстового редактора и записать в него IP-адреса СБТ, на которые необходимо произвести установку «Dr.Web для Linux». Сохранить изменения и закрыть файл (рисунок 14).

*Примечание. После записи в файл последнего значения IP-адреса необходимо нажать клавишу «Enter».*



*Рисунок 14. Редактирование файла «hosts.txt»*

5. Скопировать в каталог /root/Desktop/drw\_install\_script файл открытого ключа шифрования drwcsd.pub с сервера централизованной защиты, который располагается в каталоге /opt/drwcs/Installer/.

6. Если это первый запуск и в каталоге /root/Desktop/drw\_install\_script отсутствует архив DRW11\_Linux\_Workstations.tar.gz, то сначала необходимо выполнить команду:

```
./deploy.sh init
```

затем

```
./deploy.sh <IP_адрес_сервера_централизованной_защиты>  
<путь_к_файлу_открытого_ключа_шифрования>
```

7. По запросу скрипта сетевой установки ввести root-пароль для доступа к СВТ по ssh.

8. После завершения работы скрипта будут созданы файлы, показанные в перечне 1:

<b>result_YYYYMMDD_HHMMSS<sup>8</sup>.log</b>
Результаты работы скрипта сетевой установки в формате таблицы, состоящей из трех столбцов со следующими заголовками: 1) STATION NAME (имя станции), 2) RESULT (общий статус установки) – возможные значения: OK – установка прошла успешно, станция подключена к серверу централизованной защиты. OK/ERROR – установка прошла успешно, но возникли проблемы при подключении к серверу централизованной защиты. ERROR – при установке возникли ошибки, подробное описание которых приведено в столбце NOTES. 3) NOTES (примечания) – описание ошибки, возникшей при установке.
<b>deploy_YYYYMMDD_HHMMSS.log</b>
Общий лог работы скрипта сетевой установки
<b>IP-адрес-станции_DRW_WKS_setup.log</b>
Лог установки антивируса, скопированный со станции
<b>devel_logs/devel_YYYYMMDD_HHMMSS_IP-адрес-станции.log</b>
Отладочные логи работы скрипта сетевой установки, необходимые для выявления причин возникновения ошибок в работе.

#### *Перечень 1. Файлы работы скрипта сетевой установки*

9. Убедиться в успешном завершении процесса установки «Dr.Web для Linux» на указанные в файле hosts.txt СБТ, открыв в текстовом редакторе файл /root/Desktop/drw\_install\_script/result\_YYYYMMDD\_HHMMSS.log.

В случае некорректной установки «Dr.Web для Linux» на каком-либо СБТ в папке /root/Desktop/drw\_install\_script/deploy\_logs/ будет создан файл IP-адрес-станции\_DRW\_WKS\_setup.log, содержащий информацию об ошибке.

10. В центре управления сервера централизованной защиты, перейти на вкладку «Антивирусная сеть», открыть группу Everyone и убедиться, что статус станций «online».

## **5.2. Локальная установка**

### **5.2.1. С использованием скриптов**

Для установки «Dr.Web для Linux» с использованием скриптов необходимо:

10. Войти в систему под учетной записью суперпользователя (root).

11. Скопировать архив DRW11\_Linux\_Workstations.tar.gz и файл с контрольной суммой (DRW11\_Linux\_Workstations.tar.gz.md5) на рабочий стол (каталог /root/Desktop/).

12. Перейти в директорию рабочего стола и проверить контрольную сумму установочного файла, выполнив команды:

```
cd /root/Desktop
md5sum DRW11_Linux_Workstations.tar.gz
cat DRW11_Linux_Workstations.tar.gz.md5
```

<sup>8</sup> YYYYMMDD\_HHMMSS – соответственно, год, месяц, день, часы, минуты и секунды

Выводы команд md5sum и cat должны совпадать, в противном случае целостность установочного файла нарушена и необходимо повторно скопировать указанные выше файлы.

13. Скопировать с сервера централизованной защиты файл открытого ключа шифрования drwcsd.pub, который располагается в каталоге /opt/drwcs/Installer/.

14. Запустить консоль «Fly-терминал»: Пуск → Утилиты → Терминал Fly.

15. Перейти в каталог /root/Desktop/ и распаковать архив DRW11\_Linux\_Workstations\_install\_script.tar.gz. Для этого ввести следующие команды:

```
cd /root/Desktop/  
tar -xzf DRW11_Linux_Workstations_install_script.tar.gz
```

16. Перейти в каталог drw\_install\_script, выполнив в терминале команду:  
cd drw\_install\_script

17. Выполнить команду  
./drw\_setup.sh <IP\_адрес\_сервера\_централизованной\_защиты>  
<путь\_к\_файлу\_открытого\_ключа\_шифрования\_сервера\_централизованно  
й\_защиты>

например,

```
./drw_setup.sh 192.168.77.128 /root/Desktop/drwcsd.pub
```

В процессе выполнения файла-скрипта осуществляется:

*установка «Dr.Web для Linux»;*

*перевод «Dr.Web для Linux» в режим централизованной защиты;*

*настройка SpIDer Guard (файловый монитор) для перехвата событий  
доступа к файлам с любым уровнем привилегий;*

*настройка антивируса для корректного запуска на любом уровне  
привилегий;*

*настройка автоматической проверки usb-носителей  
при их подключении к СБТ.*

По завершении установки на экран будет выведена строка:

```
[OK] Dr.Web for Linux 11 installation is complete.
```

14. Убедиться в том, что рабочая станция успешно установила связь с сервером централизованной защиты, подключившись через веб-браузер Mozilla Firefox к центру управления и открыв вкладку «Антивирусная сеть» → Everyone (статус рабочей станции – онлайн).

15. В случае возникновения ошибок проанализировать файл DRW\_WKS\_setup.log в каталоге /root/Desktop/drw\_install\_script/

### **5.2.2. С использованием скриптов без подключения к серверу централизованной защиты**

Для установки «Dr.Web для Linux» с использованием скриптов необходимо:

1. Войти в систему под учетной записью суперпользователя (root).

2. Скопировать архив DRW11\_Linux\_Workstations.tar.gz и файл с контрольной суммой (DRW11\_Linux\_Workstations.tar.gz.md5) на рабочий стол (каталог /root/Desktop/).

3. Перейти в директорию рабочего стола и проверить контрольную сумму установочного файла, выполнив команды:



```
cd /root/Desktop
md5sum DRW11_Linux_Workstations.tar.gz
cat DRW11_Linux_Workstations.tar.gz.md5
```

Выводы команд `md5sum` и `cat` должны совпадать, в противном случае целостность установочного файла нарушена и необходимо повторно скопировать указанные выше файлы.

4. Запустить консоль «Fly-терминал»: Пуск → Утилиты → Терминал Fly.

5. Перейти в каталог `/root/Desktop/` и распаковать архив `DRW11_Linux_Workstations_install_script.tar.gz`. Для этого ввести следующие команды:

```
cd /root/Desktop/
tar -xzf DRW11_Linux_Workstations_install_script.tar.gz
```

6. Перейти в каталог `drw_install_script`, выполнив в терминале команду:

```
cd drw_install_script
```

7. Выполнить команду

```
./drw_setup.sh offline
```

В процессе выполнения файла-скрипта осуществляется:

*установка «Dr. Web для Linux»;*

*настройка SpIDer Guard (файловый монитор) для перехвата событий доступа к файлам с любым уровнем привилегий;*

*настройка антивируса для корректного запуска на любом уровне привилегий;*

*настройка автоматической проверки usb-носителей при их подключении к СБТ.*

По завершении установки на экран будет выведена строка:

```
[OK] Dr.Web for Linux 11 installation is complete.
```

8. В случае возникновения ошибок проанализировать файл `DRW_WKS_setup.log` в каталоге `/root/Desktop/drw_install_script/`

### 5.2.3. Вручную

#### 5.2.3.1 Установка «Dr.Web для Linux»

Для установки «Dr. Web для Linux» с использованием инсталляционного файла необходимо:

1. Войти в систему под учетной записью суперпользователя (`root`).

2. Скопировать архив `DRW11_Linux_Workstations.tar.gz` и файл с контрольной суммой (`DRW11_Linux_Workstations.tar.gz.md5`) на рабочий стол (каталог `/root/Desktop/`).

3. Перейти в директорию рабочего стола и проверить контрольную сумму установочного файла, выполнив команды:

```
cd /root/Desktop
md5sum DRW11_Linux_Workstations.tar.gz
cat DRW11_Linux_Workstations.tar.gz.md5
```

Выводы команд `md5sum` и `cat` должны совпадать, в противном случае целостность установочного файла нарушена и необходимо повторно скопировать указанные выше файлы.

4. Перейти в каталог `/root/Desktop/` и распаковать архив `DRW11_Linux_Workstations_install_script.tar.gz`. Для этого ввести следующие команды:

```
cd /root/Desktop/
```

```
tar -xzvf DRW11_Linux_Workstations_install_script.tar.gz
```

5. Перейти в каталог `drw_install_script`, выполнив в терминале команду:

```
cd drw_install_script
```

6. Запустить консоль «Fly-терминал»: Пуск → Утилиты → Терминал Fly.

7. Перейти в каталог `/root/Desktop/` выполнить команды для автоматической установки «Dr.Web для Linux»:

```
chmod +x drweb-workstations_11.0.2-1703021323+mo-  
linux_amd64.run  
./drweb-workstations_11.0.2-1703021323+mo-linux_amd64.run --  
-n
```

8. Учитывая специфику работы сегмента сети, на машинах которого устанавливается «Dr.Web для Linux», для бесконфликтной работы с доменом Astra Linux (ALD) и снижения нагрузки на АРМ пользователей необходимо удалить некоторые из установленных компонентов. Для этого ввести команду в терминале:

```
/opt/drweb.com/bin/zypper -n remove drweb-gated drweb-dws  
drweb-cloudd drweb-firewall drweb-netcheck drweb-httpd-bin drweb-  
httpd-linkchecker
```

### 5.2.3.2 Подключение к серверу централизованной защиты

Для подключения АРМ к серверу централизованной защиты необходимо:

1. Войти в систему под учетной записью суперпользователя (root).

2. Скопировать с сервера централизованной защиты файл открытого ключа шифрования `drwcsd.pub`, который располагается в каталоге `/opt/drwcs/Installer/`.

3. Выполнить в терминале команду:

```
drweb-ctl esconnect <IP-адрес сервера> --Key  
/root/Desktop/drwcsd.pub
```

Успешное подключение показано на рисунке 15.

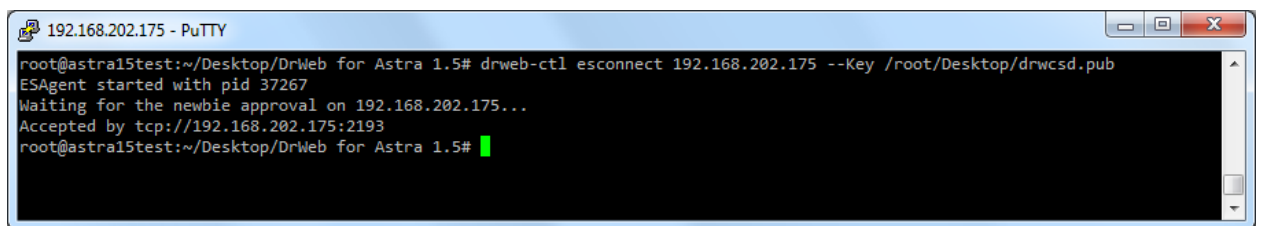


Рисунок 15. Успешное подключение станции к серверу централизованной защиты

В случае возникновения проблем с подключением к серверу централизованной защиты выполняется повторная попытка через 60 секунд, затем процесс подключения завершается и переходит в фоновый режим выполнения. Процесс подключения можно посмотреть в графическом интерфейсе САВЗ в «Настройках» на вкладке «Режим».

Для принудительного завершения процесса подключения необходимо использовать команду `drweb-ctl esdisconnect`.

*Примечание: при возникновении проблем с подключением для запуска новой попытки подключения к серверу централизованной защиты необходимо сначала ввести команду `drweb-ctl esdisconnect` и только потом снова запускать команду `drweb-ctl esconnect`.*

Если все пункты установки были выполнены правильно, то в разделе «Антивирусная защита» сервера централизованной защиты отобразится станция, на которую производилась установка (рисунок 16).

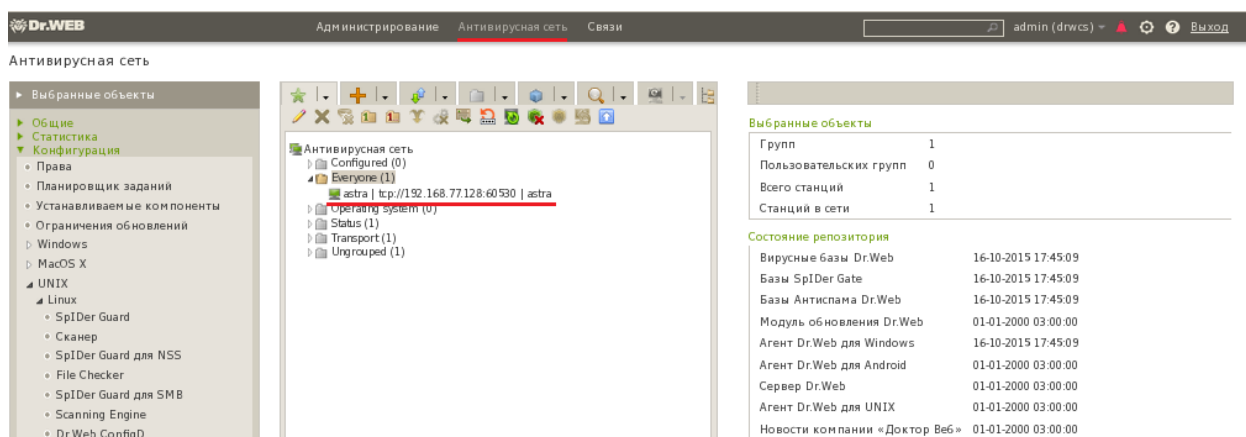


Рисунок 16. Успешно подключенная станция

### 5.2.3.3 Настройка SpIDer Guard для перехвата событий доступа к файлам с любым уровнем привилегий

«Dr.Web для Linux» в режиме работы по умолчанию не может перехватывать события о доступе к файлам с более высокими уровнями привилегий, нежели уровень привилегий, на котором запущен SpIDer Guard. Кроме того, в случае, если пользователь работает на отличном от нуля уровне привилегий, графический интерфейс «Dr.Web для Linux» не может взаимодействовать со SpIDer Guard (файловый монитор) и сервисными компонентами антивируса, работающими на других уровнях привилегий.

Для предоставления файловому монитору SpIDer Guard возможности обнаруживать доступ к файлам, имеющим любой уровень привилегий доступа, необходимо перевести SpIDer Guard в режим работы LKM.

Чтобы перевести SpIDer Guard в режим работы LKM, выполните следующие действия:

1. Войти в систему под учетной записью суперпользователя (root).
2. Запустить консоль «Fly-терминал»: Пуск → Утилиты → Терминал Fly.
3. Выполнить команду  
`drweb-ctl cfset LinuxSpider.Mode LKM`

#### 5.2.3.4 Настройка «Dr.Web для Linux» для корректного запуска на любом уровне привилегий

Чтобы все компоненты антивируса (сканер, файловый монитор SpIDer Guard, графический интерфейс и утилита управления из командной строки) корректно взаимодействовали между собой при их запуске на разных уровнях привилегий, необходимо внести изменения в сценарий запуска демона управления конфигурацией «Dr.Web для Linux» (drweb-configd) – сервисного компонента продукта, обеспечивающего взаимодействие всех антивирусных компонентов между собой.

Для этого выполните следующие действия:

1. Войти в систему под учетной записью суперпользователя (root).
2. В любом текстовом редакторе открыть файл сценария /etc/init.d/drweb-configd.
3. Найти в этом файле определение функции start\_daemon, в которой заменить строку  
"\$DAEMON" -d -p "\$PIDFILE" >/dev/null 2>&1  
на строку  
exescaps -c 0x100 -- "\$DAEMON" -d -p "\$PIDFILE" >/dev/null 2>&1
4. Сохранить изменения и перезапустить службу drweb-configd, выполнив команду /etc/init.d/drweb-configd restart

### 5.2.3.5 Настройка автоматического сканирования подключаемых usb-носителей

Для автоматической проверки подключаемых usb-носителей «Dr.Web для Linux» необходимо:

1. Войти в систему под учетной записью суперпользователя (root).
2. Скопировать архив DRW11\_Linux\_Workstations.tar.gz и файл с контрольной суммой (DRW11\_Linux\_Workstations.tar.gz.md5) на рабочий стол (каталог /root/Desktop/).

3. Перейти в директорию рабочего стола и проверить контрольную сумму установочного файла, выполнив команды:

```
cd /root/Desktop
md5sum DRW11_Linux_Workstations.tar.gz
cat DRW11_Linux_Workstations.tar.gz.md5
```

Выводы команд md5sum и cat должны совпадать, в противном случае целостность установочного файла нарушена и необходимо повторно скопировать указанные выше файлы.

4. Перейти в каталог /root/Desktop/ и распаковать архив DRW11\_Linux\_Workstations\_install\_script.tar.gz. Для этого ввести следующие команды:

```
cd /root/Desktop/
tar -xzf DRW11_Linux_Workstations_install_script.tar.gz
```

5. Перейти в каталог /root/Desktop/drw\_install\_script/extra/, выполнив команду cd /root/Desktop/drw\_install\_script/extra/.

6. Скопировать файлы 71-drweb.rules в папку /etc/udev/rules.d/, выполнив команду cp 71-drweb.rules /etc/udev/rules.d

7. Создать папку scripts в каталоге /etc/udev/scripts, выполнив команду mkdir /etc/udev/scripts

8. Скопировать файл scan-drweb.sh в папку /etc/udev/scripts/, выполнив команду cp scan-drweb.sh /etc/udev/scripts

9. Скопировать файл fly-scan-drweb.desktop в каталог /etc/xdg/autostart/, выполнив команду cp fly-scan-drweb.desktop /etc/xdg/autostart

10. Скопировать файл fly-scan-drweb в каталог /usr/bin/, выполнив команды:

```
cp fly-scan-drweb /usr/bin
chmod +x /usr/bin/fly-scan-drweb
```

## 6. Установка и настройка «Агент Dr.Web для Windows»

«Агент Dr.Web для Windows» устанавливается на СБТ под управлением ОС Windows (при наличии таких СБТ), функционирующее в ЛВС.

Установка «Агент Dr.Web для Windows» производится автономно на каждом СБТ.

Для этого необходимо:

1. Загрузить с соответствующих FTP-серверов исполняемый файл `drweb-esuite-agent-full-10.00.1-201703021-windows.exe`, с сервера централизованной защиты загрузить файл открытого ключа шифрования `drwcsd.pub`, который располагается в каталоге `/opt/drwcs/Installer/`.

2. Записать загруженные файлы на машинный носитель информации.

3. Зайти в ОС под учетной записью с правами локального администратора.

4. Перед началом установки временно отключить Брандмауэр Windows.

5. Скопировать вышеуказанные файлы на рабочий стол СБТ, на котором предполагается произвести установку «Агент Dr.Web для Windows».

6. Запустить исполняемый файл.

7. Ввести IP адрес сервера централизованной защиты, указать путь к файлу открытого ключа `drwcsd.pub` и нажать кнопку «Далее» (рисунок 17).

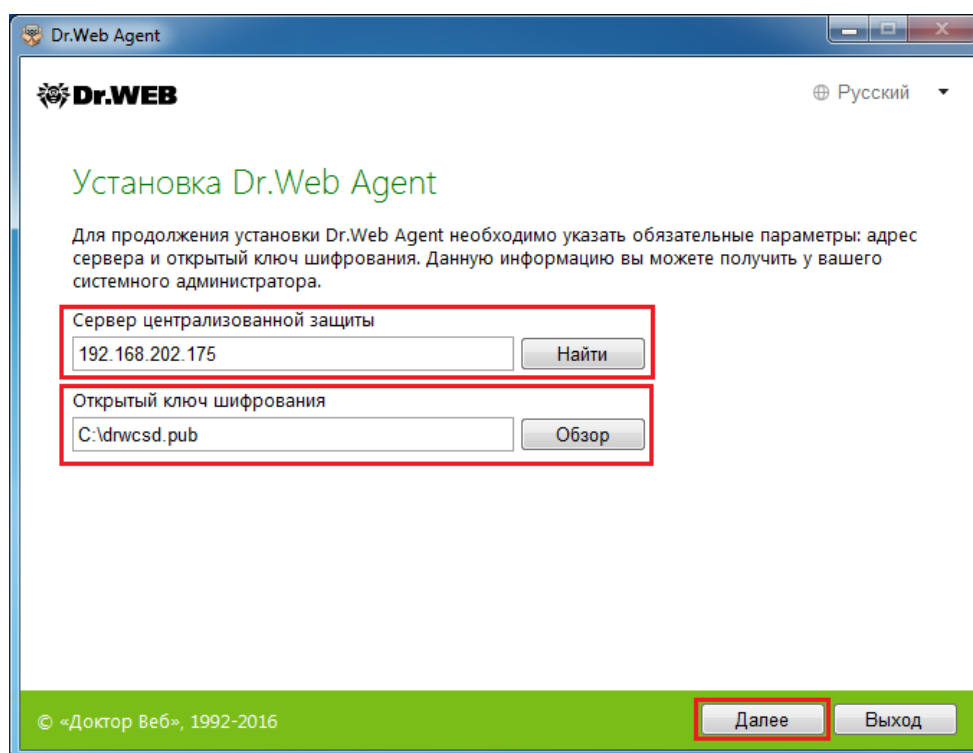


Рисунок 17. Указание IP-адреса и открытого ключа шифрования сервера централизованной защиты

8. Нажать на ссылку «Параметры установки» (рисунок 18).

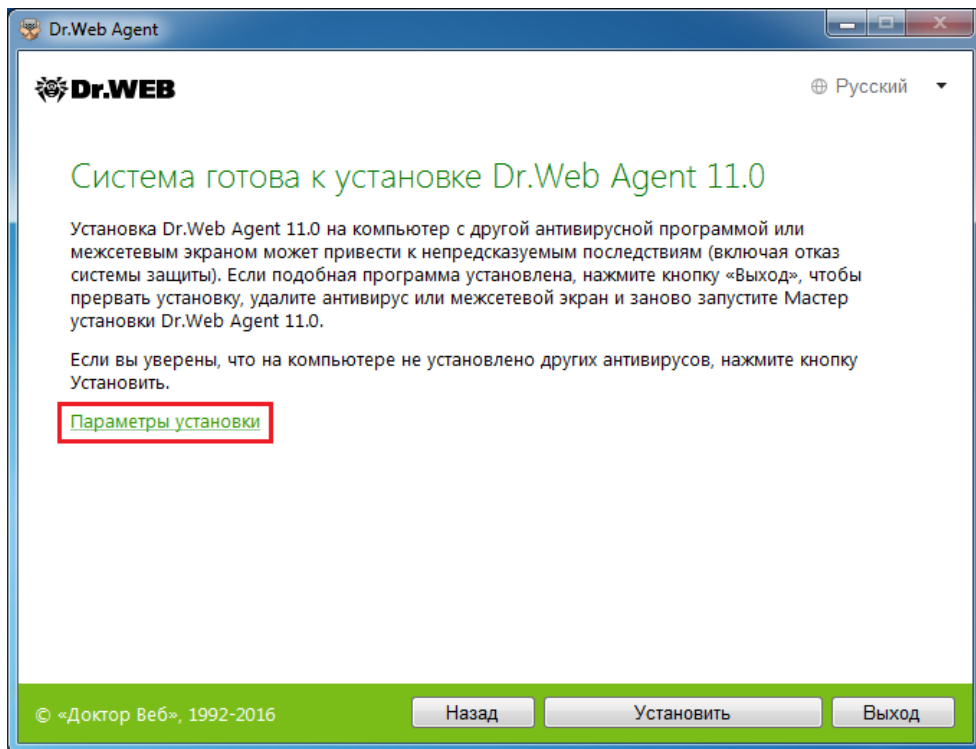


Рисунок 18. Переход в окно настроек параметров установки сервера централизованной защиты

9. Поставить галочки напротив компонентов Сканер и SpIDer Guard, напротив остальных компонентов – убрать. Далее перейти в раздел «Дополнительные опции» (рисунок 19).

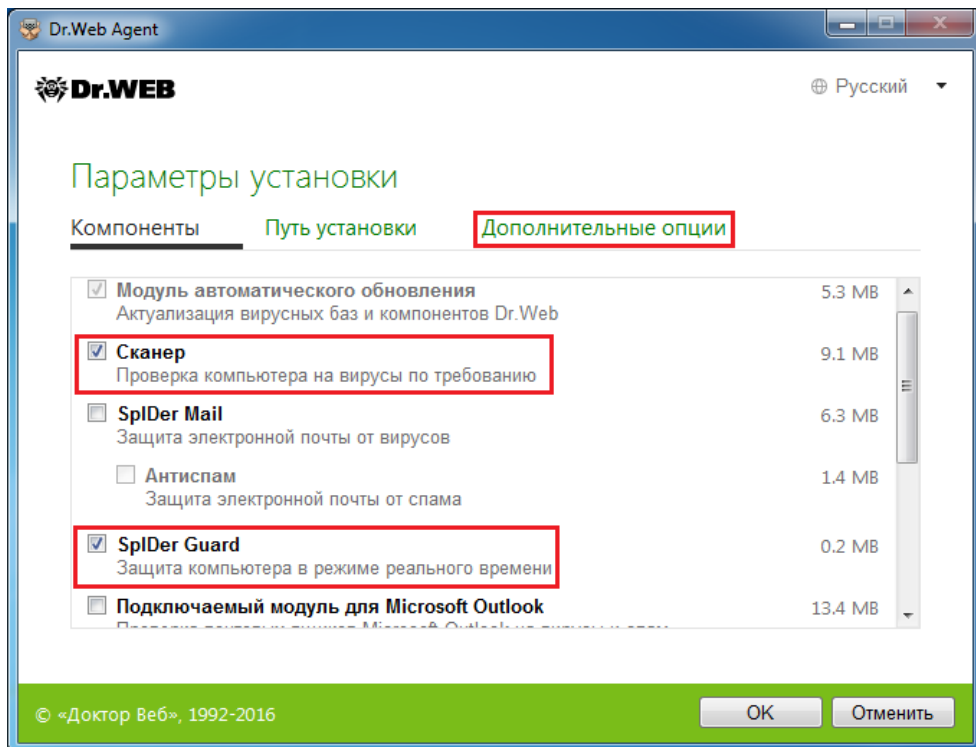
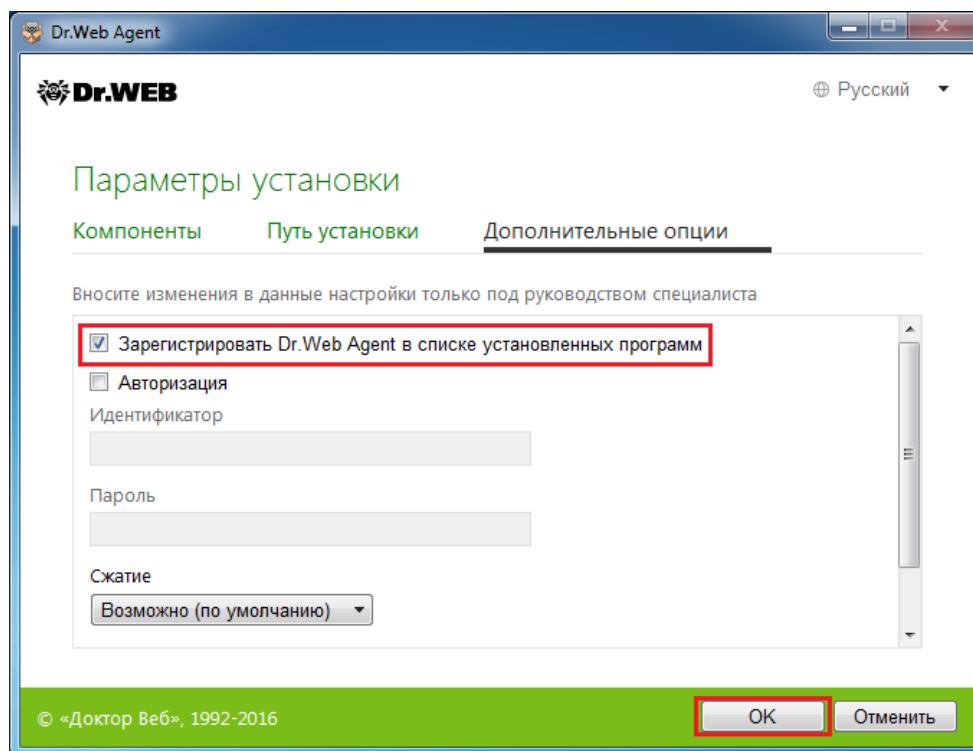


Рисунок 19. Выбор устанавливаемых компонентов продукта «Агент Dr.Web для Windows»

10. Поставить галочку напротив строки «Зарегистрировать Dr.Web Agent в списке установленных программ» и нажать кнопку «ОК» (рисунок 20).



*Рисунок 20. Настройка дополнительных опций установки  
«Агент Dr.Web для Windows»*

11. После завершения установки нажать кнопку «Перезагрузить сейчас».

После перезагрузки в разделе «Антивирусная сеть» сервера централизованной защиты появится новая станция, соответствующая СБТ, на котором произведена установка «Агент Dr.Web для Windows».



## 7. Журнал подключения и сканирования usb-носителей

При подключении usb-носителей «Dr.Web для Linux» запускает их автоматическую антивирусную проверку и записывает в журнал информацию о следующих событиях:

- время подключения и серийный номер usb-носителя;
- ход и результаты антивирусной проверки.

Журнал располагается по следующему пути:

`/var/log/drweb_check/drweb_media_scan.log`

Данный журнал ротится (создается копия журнала с другим именем и помещается в архив) ежемесячно. Может храниться до 12 копий журналов (за весь год).

Пример содержания журнала при проверке usb-носителя:

```
20.03.2018      11:11:43      Съемный      носитель
Flash_Drive_AU_USB20_I87B5771 подключен.
Begin_scan
/media/sdc_I87B5771_drw_scan/FOUND.000/FILE0000.CHK - Ok
.
.
.
/media/sdc_I87B5771_drw_scan/scan & print/img-110072421.pdf
(PDF) - Ok
Scanned objects: 155, scan errors: 3, threats found: 0,
threats neutralized: 0.
Scanned 184136.05 KB in 27.38 s with speed 6724.96 KB/s.
End_scan
20.03.2018      11:12:12      Сканирование      съемного      носителя
Flash_Drive_AU_USB20_I87B5771 завершено.
```

## 8. Действия при возникновении ошибок

При возникновении ошибок при работе скрипта установки и настройки сервера централизованной защиты (drw\_ess\_install.sh) и скрипта установки и настройки «Dr.Web для Linux» (drw\_setup.sh) необходимо проанализировать файлы журналов, перечисленные в перечне 2, на наличие ошибок.

<b>Скрипт установки и настройки сервера централизованной защиты</b>
Каталог /root/Desktop/drw_ess_install_script/ Файл DRW_ESS_setup.log
<b>Скрипт установки и настройки «Dr.Web для Linux»</b>
Каталог /root/Desktop/drw_install_script/deploy_logs/ Файлы: <ul style="list-style-type: none"><li>• result_YYYYMMDD_HHMMSS<sup>9</sup>.log</li><li>• deploy_YYYYMMDD_HHMMSS.log</li><li>• IP-адрес-станции_DRW_WKS_setup.log (при наличии)</li></ul> Каталог /root/Desktop/drw_install_script/deploy_logs/devel_logs/ Файл devel_YYYYMMDD_HHMMSS_IP-адрес-станции.log

*Перечень 2. Файлы журналов, необходимые для анализа ошибок, возникших при работе скриптов*





<sup>9</sup> Примечание: YYYYMMDD\_HHMMSS – соответственно, год, месяц, день, часы, минуты и секунды.

## 9. Проверка правильности настроек

В данном разделе приведены настройки, которые необходимо проверить, чтобы убедиться в корректности настройки сервера централизованной защиты Dr.Web для Linux.

### 9.1. Сервер централизованной защиты

Все контрольные параметры проверяются с помощью центра управления сервера централизованной защиты, который доступен по адресу <http://IP:9080> (где IP – адрес сервера централизованной защиты) и отражены в таблице 3.

№ п/п	Проверяемый параметр	Значение	Расположение
1.	Версия сервера Dr.Web	10.00.1 (11-02-2017 03:00:00)	Администрирование > Менеджер лицензий
2.	Лицензионный ключ	Действителен и распространен на группу Everyone  <b>Ключи</b>  GK17-ES20000-13-12 - 10-07-2018 14:32:14  Everyone	
3.	Название Сервера Dr.Web	Задано имя <sup>10</sup> сервера централизованной защиты	Администрирование > Конфигурация Сервера Dr.Web > Общие
4.	Режим регистрации новичков	Автоматически разрешать доступ	
5.	Все параметры раздела «Модули»	Установлены все галочки напротив каждой строки раздела «Модули»: 	Администрирование > Конфигурация Сервера Dr.Web > Модули
6.	Параметр «Использовать SSL»	Установлена галочка напротив данного параметра	Администрирование > Удаленный доступ к серверу Dr.Web
7.	Адрес	127.0.0.1	
8.	Адрес	IP-адрес сервера централизованной защиты	
9.	Задача «Ежедневная перезагрузка сервера»	Присутствует в списке со следующими параметрами: Состояние – Разрешено Серьезность – Критический Периодичность – Ежедневно в 23:00 Действие – Перезапуск Сервера Dr.Web	Администрирование > Планировщик заданий Сервера Dr.Web
10.	Задачи по-умолчанию	Минимальное количество задач и их параметры показаны на рисунке 21. Должны отсутствовать задачи по умолчанию, названия которых начинаются на «Update...»	
11.	Вирусные базы Dr.Web	В столбце «Текущая ревизия» отображается актуальная дата (не старше недели)	Администрирование > Состояние репозитория
12.	Задачи по расписанию для группы Everyone	Минимальное количество задач и их параметры показаны на рисунке 22	Антивирусная сеть > Everyone > Планировщик заданий

<sup>10</sup> Имя сервера определяется из названия позывного узла связи и условного наименования воинской части. Например, для воинской части 12345, позывной узла связи Зарево, имя сервера Zarevo\_12345



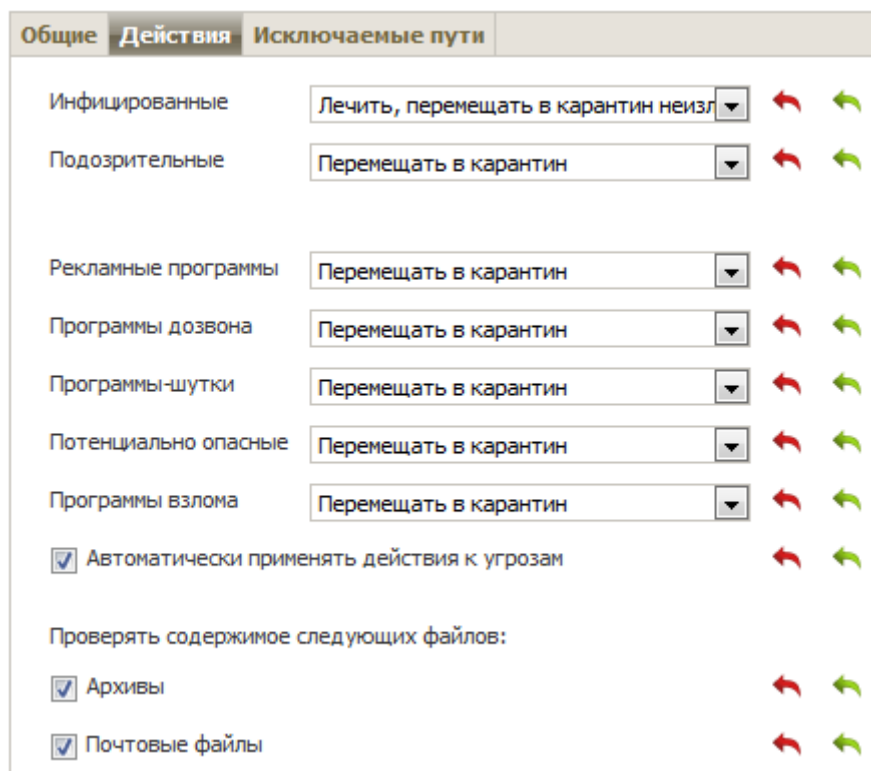


Рисунок 24. Требуемые действия для различных типов обнаруженных объектов для компонента Сканер

## 9.2. «Dr.Web для Linux»

Часть параметров можно проверить как с помощью центра управления сервера централизованной защиты, который доступен по адресу <http://IP:9080> (где IP – адрес сервера централизованной защиты), так и локально на самой станции. Другую часть параметров необходимо проверять на самой станции, или удаленно подключившись к ней по протоколу ssh.

№ п/п	Проверяемый параметр	Значение	Расположение
1.	Подключение к серверу централизованной защиты	Станция отображается в списке группы Everyone и слева от названия станции виден зелёный значок монитора (на рисунке станция astra выключена, а astra15test включена)  Антивирусная сеть Everyone (2) astra   tcp://192.168.202.167:52862 astra15test   tcp://192.168.202.175:39278 Status (2) Transport (1) Ungrouped (2)	Антивирусная сеть
2.	Установленные компоненты	Минимальный набор установленных компонентов показан на рисунке 25	Антивирусная сеть > <имя-станции> > Установленные компоненты
3.	Запущенные компоненты	Минимальный набор запущенных компонентов показан на рисунке 26	Антивирусная сеть > <имя-станции> > Запущенные компоненты

4.	Дата выпуска БВС	<div>В столбце «Текущая ревизия» отображается актуальная дата (не старше недели)</div> <table><tr><td>Название продукта ^</td><td>Текущая ревизия</td><td>Состояние</td></tr><tr><td>Вирусные базы Dr.Web</td><td>07-03-2018 07:40:40</td><td>Состояние нормальное</td></tr></table>	Название продукта ^	Текущая ревизия	Состояние	Вирусные базы Dr.Web	07-03-2018 07:40:40	Состояние нормальное	Антивирусная сеть > <имя-станции> > Продукты
Название продукта ^	Текущая ревизия	Состояние							
Вирусные базы Dr.Web	07-03-2018 07:40:40	Состояние нормальное							
5.	Версия вирусных баз и дата выпуска файлов d*today.vdb	<div>В столбце «Версия» для всех строчек установлено значение 11. Для удобства просмотра удобно сортировать столбцы «По убыванию», нажав кнопку «Стрелочка вниз» в заголовке столбца.</div> <div>В столбце «Выпущена» для файлов dwmtoday.vdb, dwrtoday.vdb, drwtoday.vdb, dwntoday.vdb, drwdaily.vdb отображается актуальная дата (не старше недели).</div>	Антивирусная сеть > <имя-станции> > Вирусные базы						
6.	Состояние станции	Отсутствуют ошибки в таблице	Антивирусная сеть > <имя-станции> > Состояние						
7.	Проверка usb-носителей	Необходимо на самой станции (или подключившись по ssh) проверить наличие следующих файлов: /etc/udev/rules.d/71-drweb-usb.rules /etc/udev/scripts/scan_usb.sh /usr/bin/fly-scan-drweb /etc/xdg/autostart/fly-scan-drweb.desktop /etc/logrotate.d/fly-scan-drweb	Файловая система Astra Linux						

Компонент	Время установки	Сервер Dr.Web	Путь
Dr.Web ConfigD для Linux	26-01-2018 11:11:15	local	/opt/drweb.com/bin/drweb-configd.real
Scanning Engine для Linux	26-01-2018 11:11:40	local	/opt/drweb.com/bin/drweb-se
Dr.Web File Checker для Linux	26-01-2018 11:11:44	local	/opt/drweb.com/bin/drweb-filecheck
Dr.Web Agent Сканер для UNIX	26-01-2018 11:11:44	local	/opt/drweb.com/bin/drweb-filecheck
Сканер Dr.Web для Linux	26-01-2018 11:11:26	local	/opt/drweb.com/bin/drweb-gui
SpIDer Guard для Linux	26-01-2018 11:11:47	local	/opt/drweb.com/bin/drweb-spider

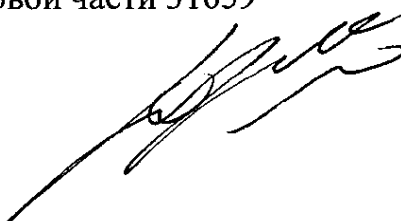
Рисунок 25. Минимальное количество установленных компонентов «Dr.Web для Linux»

<input type="checkbox"/>	Время запуска	Компонент	Тип запуска	Пользователь	Аргументы
	15-03-2018 10:12:38	Dr.Web ConfigD для Linux			
	15-03-2018 10:12:40	Scanning Engine для Linux			
	15-03-2018 10:12:40	Dr.Web File Checker для Linux			
	15-03-2018 10:12:40	SpIDer Guard для Linux			

Рисунок 26. Минимальное количество запущенных компонентов «Dr.Web для Linux»

Начальник 3 центра войсковой части 31659  
подполковник

«23» марта 2018 г.



Ю.Войнов

## Настройка взаимодействия с удаленным графическим интерфейсом Astra Linux

Для соединения с сервером централизованной защиты, установленным на Astra Linux, в зависимости от типа ОС необходимо:

### Соединение Astra Linux → Astra Linux

На сервере централизованной защиты:

1. В файле /etc/ssh/sshd\_config установить следующие параметры:

```
X11Forwarding yes
```

```
X11UseLocalhost no
```

2. Перезапустить демона ssh, выполнив в терминале команду:

```
/etc/init.d/ssh restart
```

На клиенте:

1. Подключиться к серверу централизованной защиты, используя команду:

```
ssh -X root@<IP-адрес-сервера-централизованной-защиты>
```

или

```
ssh -X <учетная-запись-пользователя-с-правами-на-выполнение-команд-супер-пользователя>@<IP-адрес-сервера-централизованной-защиты>
```

### Соединение Windows → Astra Linux

На сервере централизованной защиты (Astra Linux):

1. Запустить демон удаленного рабочего стола с помощью команды:

```
/etc/init.d/xrdp start
```

*Примечание: при отсутствии файла /etc/init.d/xrdp необходимо установить данный демон с помощью команд:*

*При наличии установочного диска с Astra Linux в DVD-приводе сервера централизованной защиты:*

```
apt-cdrom add
```

```
apt-get update
```

```
apt-get install xrdp
```

*В противном случае:*

1) Скачать с соответствующих FTP-серверов из папки xrdp deb-файлы xrdp\_0.5.0-2\_amd64.deb и vnc4server\_4.1.1+X4.3.0-37.1\_amd64.deb

2) Скопировать их на сервер централизованной защиты

3) Установить, используя команду:

```
dpkg -i vnc4server_4.1.1+X4.3.0-37.1_amd64.deb xrdp_0.5.0-2_amd64.deb
```

На клиенте (Windows):

1. Запустить утилиту «Подключение к удаленному рабочему столу» (mstsc.exe).

2. Подключиться к серверу централизованной защиты под учетной записью суперпользователя.

### Команды скриптов для удаления соответствующих САВЗ

У скриптов автоматической установки и настройки сервера централизованной защиты и сетевой установки «Dr.Web для Linux» есть параметры командной строки для их удаления.

1. Удаление сервера централизованной защиты выполняется с помощью ключа командной строки `uninstall`

```
./drw_ess_setup.sh uninstall
```

В ходе работы данной команды выполняется:

1) Удаление сервера централизованной защиты **без создания резервной копии** сервера централизованной защиты.

2) Удаление плагина для браузера Mozilla Firefox.

2. Удаление «Dr.Web для Linux» выполняется с помощью ключа командной строки `uninstall`

```
./drw_setup.sh uninstall
```

В ходе работы данной команды выполняется:

1) Отключение машины от сервера централизованной защиты.

2) Удаление САВЗ «Dr.Web для Linux».

3) Удаление скрипта запуска антивирусной проверки подключаемых usb-носителей.

4) Удаление правила монтирования подключаемых usb-носителей для запуска антивирусной проверки.

5) Завершение демона, отображающего уведомление о начале и окончании антивирусной проверки usb-носителей (далее – демон).

6) Удаление демона из списка автозагрузки.

7) Удаление файла скрипта демона.