

Руководство

 **AntiVir**<sup>®</sup>  
SharePoint

---

## Copyright information

The purpose of this information is to acknowledge and recognize the code from third-party suppliers used for Avira

AntiVir SharePoint. We would like to thank the copyright owners for allowing us to use their code.

### **MD5 Code**

The MD5 code used for security reasons was written by the Information Science Institute of the University of Southern

California and derived from the Message-Digest algorithm from RSA Data Security, Inc. Copyright (C) 1991-2, RSA Data Security, Inc. Created in 1991.

All rights reserved.

The license to copy and use this software is distributed with the stipulation that it is designated as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all materials mentioned by this software or which refer to this software or these functions.

The license is also granted for the creation of works deriving from this, with the stipulation that these works are

designated as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all materials which mention the derived work or refer to it.

RSA Data Security, Inc. provides no warranty whatsoever regarding the marketability of this software or the suitability of this software for a particular purpose. It is provided without any guarantee in its present form. This applies to expressed

or implied guarantees.

This information must be contained in every copy of each part of this documentation and/or software.

---

# Содержание

<b>1 Введение .....</b>	<b>4</b>
<b>2 Символы .....</b>	<b>5</b>
<b>3 Информация о продукте .....</b>	<b>6</b>
3.1 Обзор .....	6
3.2 Функции .....	7
3.3 Системные требования .....	7
3.4 Лицензирование .....	8
<b>4 Установка и удаление.....</b>	<b>9</b>
4.1 Установка.....	9
4.2 Удаление .....	10
<b>5 Пользовательский интерфейс и управление .....</b>	<b>11</b>
5.1.1 Пользовательский интерфейс .....	11
5.1.2 Управление.....	11
<b>6 Обнаружение вирусов.....</b>	<b>12</b>
<b>7 Статус .....</b>	<b>13</b>
7.1.1 .....	13
7.1.2 .....	14
7.1.3 Последнее обновление .....	15
7.1.4 Последний вирус.....	16
<b>8 Настройки.....</b>	<b>18</b>
8.1 Настройки AntiVir.....	18
8.2 Антивирусные настройки SharePoint .....	20
8.3 Настройка обновлений .....	21
<b>9 Обновления .....</b>	<b>24</b>
<b>10 Информация и сервис.....</b>	<b>25</b>
10.1.1 Подозрительные файлы.....	25
10.1.2 Ложные срабатывания.....	25

# 1 Введение

Avira AntiVir SharePoint компании Avira GmbH является антивирусным решением, специально разработанным для Microsoft SharePoint, позволяющим предотвратить распространение вирусов и другого вредоносного ПО через страницы SharePoint Team.

Вирусы, вредоносное ПО и нежелательные программы в данном руководстве будут называться вирусами.



Данное руководство описывает процесс установки и использования программы.

На нашем сайте <http://www.avirus.ru> Вы сможете загрузить руководство по Avira AntiVir SharePoint в виде файла PDF file.

Команда Avira GmbH team

## 2 СИМВОЛЫ

Используются следующие символы:

Символ	Описание
✓	Обязательное условие
▶	Действие
	Предупреждение об опасности
	Важная информация

### 3 Информация о продукте

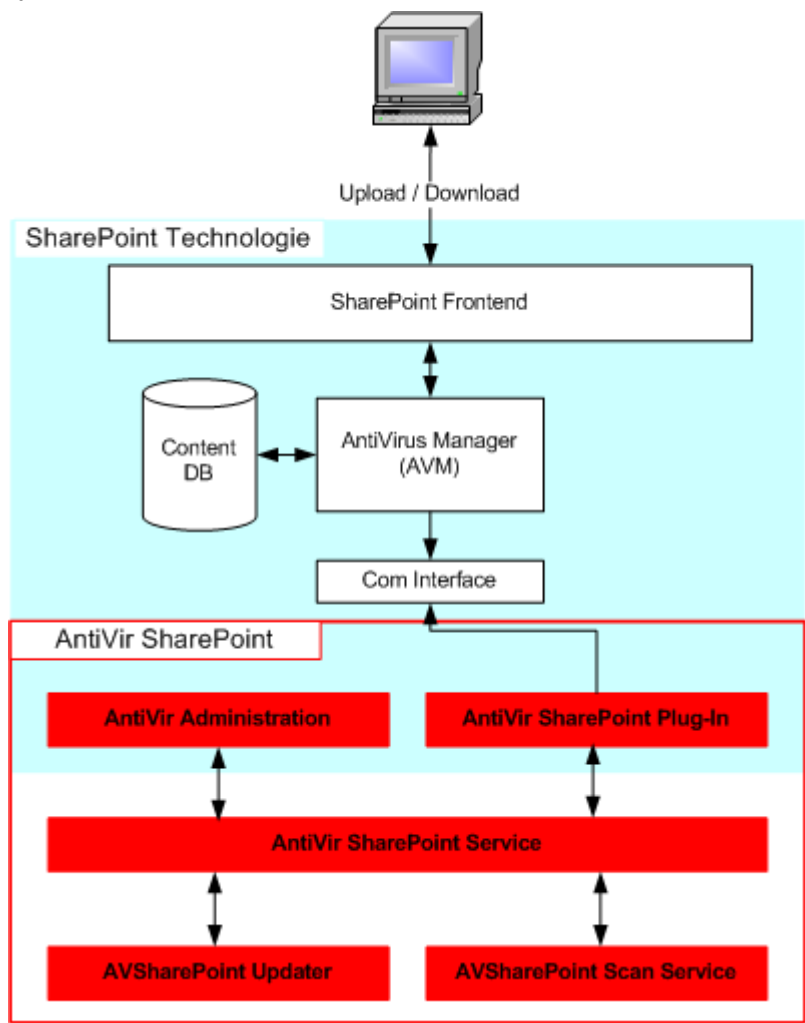
#### 3.1 Обзор

AntiVir SharePoint – это антивирусное решение, которое специально разработано для Microsoft SharePoint и поддерживает Microsoft SharePoint Services и Microsoft SharePoint Portal Server 2003.

Технология Microsoft SharePoint позволяет пользователям получать доступ к документам компании из центрального хранилища. Доступ осуществляется через web-интерфейс – the SharePoint Team pages – посредством выгрузки и загрузки документов. Документы или файлы хранятся в центральной базе данных MS SQL. Такой подход может стать проблемой безопасности, так как в этом случае данные не получится защитить стандартным антивирусным решением (постоянной проверкой или проверкой по требованию): такие методы требуют, чтобы данные были представлены в виде файлов в файловой системе.

AntiVir SharePoint сканирует документы на наличие вирусов и вредоносных программ при загрузке и выгрузке в/из SharePoint Team pages. В случае обнаружения вирусов передача документа прекращается, если лечение документа невозможно.

Архитектура:



В технологии SharePoint использование внешних антивирусных программ контролируется через Antivirus Manager (AVM). Функции антивирусной защиты могут быть включены в настройках SharePoint. AVM передает данные во внешнюю антивирусную программу.

AntiVir интегрирован в виде plug-in в SharePoint. Plug-in AntiVir SharePoint обрабатывает запросы на антивирусную проверку и перенаправляет их службе AntiVir SharePoint service. Служба AntiVir SharePoint service перенаправляет запрос службе AVSharePoint Scan service, запускает обновление AntiVir update service и предоставляет возможность настроить AntiVir. Поиск вирусов и вредоносных программ производится службой AVSharePoint scan service.

## 3.2 Функции

AntiVir SharePoint предлагает полную антивирусную защиту для данных компании, которые работают по технологии SharePoint technologies. Дополнительно Вы защищаете компьютерные системы, используемые для SharePoint.

AntiVir SharePoint легко устанавливается и имеет следующие возможности настройки:

- настройки для поиска вирусов и вредоносных программ:
  - сканирование архивов
  - эвристика макровирусов
  - эвристика WIN 32
- Настройки автоматического обновления (обновление поискового ядра и антивирусных баз):
  - обновление через файловый или веб-сервер
  - обновление, используя прокси
  - функция уведомления по эл. почте
- настройки отчетов:
  - ограничение файла отчетов

## 3.3 Системные требования

Avira AntiVir SharePoint поддерживает технологии SharePoint:

- Windows SharePoint Services
- Windows SharePoint Portal Server 2003

Системные требования:

- Службы Windows SharePoint Services или Windows SharePoint Portal Server 2003
- .NET Framework Version 2 или 3
- процессор, начиная от Intel Pentium III или x64 совместимые 64-bit процессоры
- минимум 512 MB RAM
- минимум 100 MB свободного места на жестком диске

## 3.4 Лицензирование

Для использования Avira AntiVir SharePoint Вам потребуется лицензия. Лицензия представляет собой цифровой ключ лицензии (hbedv.key). Файл лицензии содержит информацию о всех купленных продуктах AVIRA.

Во время установки программа запросит у Вас файл лицензии.

## 4 Установка и удаление

### 4.1 Установка

Перед установкой AntiVir SharePoint проверьте следующие условия:

- ✓ Соблюдаются системные требования.
- ✓ Вы используете учетную запись администратора.
- ✓ Имеется соединение с Интернетом.
- ✓ Имеется действующий файл лицензии hbedv.key, который сохранён в локальной папке.

Для того чтобы администрирование SharePoint через веб-интерфейс работало корректно, необходимо сделать следующие настройки в Internet Information Service (IIS):

- ▶ Установите значение расширения web служб .NET Framework 2.x или 3.x в значение 'Allowed'.  
Вы можете найти web service extensions в менеджере Internet Information Service Manager в разделе **Web service extensions**.
- ▶ Установите версию ASP.NET, используемую центральным администрированием SharePoint 2.x или 3.x. Перейдите в Internet Information Service Manager к **Websites :: SharePoint central administration :: Properties :: ASP.NET :: ASP.NET- Version**.



Настройки можно сделать до или после установки AntiVir SharePoint.

---

Установка Avira AntiVir SharePoint:

- ▶ Запустите файл setup.exe
- ▶ Следуйте инструкциям мастера установки
- ▶ Подтвердите остановку службы WWW publishing service.
- ▶ Подтвердите, что вы согласны с условиями лицензионного соглашения.
- ▶ Введите пользователя с правами доступа к общей папке обновлений AntiVir SharePoint update directory. Это необходимо в случае, если обновления будут производиться через файловый сервер и для файлового сервера требуются права доступа. После установки данные настройки можно будет изменить.
- ▶ Загрузите файл лицензии hbedv.key.
- ▶ Запустите установку.
- ▶ Завершите установку нажатием кнопки **Finish**.

## 4.2 Удаление

Выполните удаление через панель управления:





- ▶ **Панель управления :: Установка/удаление программ Avira AntiVir SharePoint** и кликните удалить **Remove**.
- ▶ Подтвердите удаление.

Во время удаления службы AntiVir будут остановлены, все программные файлы и логики будут удалены.

## 5 Пользовательский интерфейс и управление

### 5.1.1 Пользовательский интерфейс

Администрирование AntiVir в SharePoint основано на веб-интерфейсе.

Status		<a href="#">Help</a>	
Status information of Avira AntiVir SharePoint.			
	Info	Status	Action
 <b>AntiVir SharePoint service</b>	Connected to AntiVir SharePoint Service!	Activated	-
 <b>Sharepoint antivirus settings</b>	On up- and download	Secure	<a href="#">Change</a>
 <b>Last update</b>		11/21/2007	<a href="#">Start update</a>
	Virus definition file:	V7.00.00.241, 11/21/2007	
	Scan engine:	V7.06.00.34, 11/20/2007	
 <b>Last virus</b>	-		<a href="#">Reset</a>
	Scanned files:	0	

Доступ к управлению AntiVir можно получить через центральное администрирование SharePoint:

**Start :: Programs :: Administration :: SharePoint central administration :: AntiVir administration**

В администрировании AntiVir имеются следующие разделы:

- **Status:** информация о статусе службы AntiVir SharePoint, настройках SharePoint Antivirus и статусе AntiVir SharePoint.
- **Configuration:** страницы настроек
- **Information:** информация о текущей версии и контактной информации

### 5.1.2 Управление

AntiVir соответствует стандартам рабочего стола web (web-based desktop):

- Вы можете передвигаться в панели администрирования, используя ссылки. Команды можно выполнять ссылками или кнопками.
- Во время настройки необходимо подтверждать сделанные изменения кнопкой **ОК** внизу экрана. Настройки будут приняты без перезапуска.

## 6 Обнаружение вирусов

Во время выгрузки и загрузки документов AntiVir SharePoint сканирует их на наличие вирусов и вредоносных программ. Если AntiVir находит вирусы или вредоносные программы в документе, то передается сообщение в SharePoint. Передача документа в SharePoint будет прекращена. Пользователь увидит сообщение следующего вида:

### Virus Found

---

"eicar.com.txt" contains the following virus: "Eicar-Test-Signature".

This file cannot be saved to this document library. You must use an antivirus program to remove the virus before you save this file to the document library.



Действие при обнаружении вируса можно настроить в SharePoint anti-virus settings. Таким образом, Вы можете разрешить загрузку инфицированных файлов, чтобы пользователь сам проверил данный файл на наличие вирусов и вредоносных программ.



---

## 7 Статус

Статус и статистика отображаются в разделе **Status** :

### 7.1.1 Служба AntiVir SharePoint Service

Отображаемый статус службы AntiVir SharePoint:




Символ	Информация	Статус	Описание
	Connected to the service	Enabled	Имеется связь со службой AntiVir SharePoint service.
	No connection to the service	Disabled	Связь со службой AntiVir SharePoint service отсутствует



При отсутствии связи с AntiVir service файлы не проверяются на наличие вирусов и вредоносных программ! Проверьте, запущена ли служба AntiVir SharePoint service, при необходимости перезапустите её.

## 7.1.2 Антивирусные настройки SharePoint

Антивирусный статус SharePoint:

Символ	Информация	Статус	Действие	Описание
	Во время загрузки и выгрузки	Secure	Change	Антивирусная защита для загрузки и выгрузки включена в антивирусных настройках SharePoint. Перейти к данным настройкам можно по ссылке <b>Change</b> .
	Во время выгрузки -ИЛИ- загрузки	Not secure	Change	Антивирусная защита для выгрузки ИЛИ загрузки выключена  Перейти к данным настройкам можно по ссылке <b>Change</b> .
	Not enabled	Not secure	Change	Антивирусная защита для выгрузки и загрузки в SharePoint отключена  Перейти к данным настройкам можно по ссылке <b>Change</b> .






Если антивирусный статус *not secure*, то документы не проверяются на вирусы или вредоносные программы во время выгрузки или загрузки. Перейдите по ссылке **Change** для включения антивирусной защиты во время выгрузки и загрузки документов.

### 7.1.3 Последнее обновление

Отображается информация о последнем обновлении поискового ядра и файла вирусных сигнатур:

- Информация о статусе обновления с последней датой обновления
- Версия файла вирусных сигнатур (VDF)
- Версия поискового ядра

Символ	Статус	Действие	Описание
	Дата обновления, 05.11.2007	Start update	Последнее обновление VDF произведено менее 1 дня назад. Вы можете запустить обновление по ссылке <b>Start update</b> .
	Дата обновления, 05.11.2007	Start update	Обновление VDF произведено более 1 дня и менее 3 дней назад. Вы можете запустить обновление по ссылке <b>Start update</b> .
	Дата обновления, 05.11.2007	Start update	Последнее обновление произведено более 3 дней назад. Вы можете запустить обновление по ссылке <b>Start update</b> .





Антивирусная защита может быть эффективна только в том случае, если файлы вирусных сигнатур и поисковое ядро будут постоянно обновлены. Запустите обновление по ссылке **Start update**. Настройте функцию автоматического обновления в разделе **Configuration :: Updater configuration**.

#### 7.1.4 Последний вирус

Информация об обнаруженных вирусах:

- Последний обнаруженный вирус
- Число проверенных файлов

Символ	Информация	Статус	Описание
		Reset	нет обнаруженных вирусов
	Имя последнего вируса  Число проверенных файлов	Reset	Обнаружены вирусы Вы можете сбросить статистику перейдя по ссылке <b>Reset</b> .



## 8 Настройки

### 8.1 Настройки AntiVir

В меню **AntiVir configuration** Вы можете настроить размер файлов отчетов и поведение AntiVir SharePoint.

#### Настройки отчета

- **Limit size of the report file** (ограничить размер файла отчета)  
введите максимальный размер файла отчета в КВ. Если максимальный размер файла исчерпан, то более старые записи будут автоматически удалены! Значение по умолчанию – 1000 КВ. Данная настройка изменяет размер файла **savapi.log**. Данный файл сохраняется в следующей директории:

```
C:\Documents and Settings\All Users\Application  
Data\Avira\AntiVir SharePoint\LOGFILES
```

#### Настройки для проверки архивов

- **Scanning archives**  
Если данная опция активна, то архивы будут проверяться. Архивы будут распакованы и проверены. Проверка архивов активна по умолчанию. Рекомендуется не отключать данную опцию. Так как проверка архивов может потребовать использование значительных ресурсов компьютера, у Вас в дальнейшем есть возможность ограничения проверки архивов.
- **Smart extensions**  
Если данная опция активна, AntiVir SharePoint определяет, является ли файл архивом, даже если файл имеет нестандартное расширение, и проверяет его. Каждый файл должен быть открыт для проверки формата данных. Это снижает скорость проверки. Эта настройка включена по умолчанию и рекомендована к использованию.
- **Limit recursion depth of the scan**  
При проверке архивов AntiVir SharePoint использует рекурсивное сканирование: вложенные архивы распаковываются и проверяются на наличие вирусов и вредоносных программ. Значение глубины рекурсии может изменяться в пределах от 1 до 99. Значение по умолчанию равно 5. Например: глубина рекурсии равна 2. Все архивы, размещенные непосредственно в главном архиве будут распакованы и проверены.
- **Alarm with archive nestings via**  
Вы можете предотвратить передачу глубоко вложенных архивов. Глубоко вложенные архивы, так называемые 'архивные бомбы', являются популярным методом маскировки вирусов и заражения системы. Передача архивов, которые имеют более высокую степень вложенности, чем указано, не будут переданы через страницы SharePoint Team pages. Возможные значения от 1 до 300. Значение по умолчанию 150.
- **Maximum size of files to be scanned**  
Ограничение максимального размера проверяемого архива. Возможные значения от 1 до 600 МВ. Значение по умолчанию = 300 МВ.

---

## Расширенные настройки

### – **Macro heuristic**

AntiVir имеет мощную эвристику. Если данная опция включена, то документы будут проверены на наличие неизвестных макровирусов. В зараженном документе все макровирусы будут удалены, если лечение возможно.

### – **Win 32 heuristic**

AntiVir имеет мощный эвристический анализатор по поиску вирусов, червей и Троянов и может находить неизвестные формы данного вредоносного ПО. Если данная опция включена, то Вы можете выбрать "строгость" эвристической проверки:

#### **Detection level low**

AntiVir обнаруживает меньше вредоносных программ, риск ложных срабатываний минимален.

#### **Detection level medium**

Данная настройка установлена по умолчанию.

#### **Detection level high**

AntiVir обнаруживает большое число неизвестного вредоносного ПО, но возможны и ложные срабатывания.

## 8.2 Антивирусные настройки SharePoint

В меню **SharePoint *Anti-virus settings*** Вы можете сделать антивирусные настройки для SharePoint Antivirus Manager. При помощи SharePoint Antivirus Manager Вы можете контролировать поведение используемой антивирусной программы:

- **Scan documents during upload**

Документы проверяются на вирусы во время выгрузки, т.е. до сохранения в базе данных SharePoint.

- **Scan documents during download**

Документы проверяются на вирусы до загрузки.

- **Allow users to download infected documents**

Разрешена загрузка документов, даже если документ инфицирован. Пользователи сами должны проверять антивирусной программой загруженные документы на наличие вирусов и другого вредоносного ПО .

- **Attempt to clean infected files**

AntiVir SharePoint пытается удалить вредоносное ПО из зараженного документа. Если вредоносное ПО может быть успешно удалено, то передача из/в SharePoint Team будет разрешена.

- **Virus scan timeout after n seconds**

Введите время ожидания в секундах для проверки на вирусы. Значение по умолчанию 300 секунд.

- **Permissible thread number for virus scanner**

Введите разрешенное число потоков для антивирусной проверки.



Настройки антивирусной защиты применяются на странице SharePoint. Ссылка на данную страницу доступна только из AntiVir. Информация по индивидуальным опциям настройки доступна в секции Help Microsoft SharePoint.

Вы также можете попасть на антивирусные настройки SharePoint через центральное администрирование SharePoint:

- ▶ Перейдите к следующим настройкам Windows SharePoint central administration: Security configuration :: Configure anti-virus settings
-

## 8.3 Настройка обновлений

На странице **Updater configuration** Вы можете указать сетевые настройки и при необходимости настройки проху для автоматического обновления AntiVir SharePoint. Здесь можно также настроить рассылку уведомлений по электронной почте, используя протокол SMTP.

### Network settings (сетевые настройки)

Обновления можно получать через web-сервер или через файловый сервер / общую папку из Интернета или локальной сети.

#### – Update URL

Введите адрес URL или адрес IP того сервера, с которого Вы собираетесь скачивать обновления. Можно ввести несколько адресов web-серверов, разделенных запятыми. AntiVir SharePoint использует первый доступный сервер для обновления:

```
http://dl1.pro.antivir.de/upd,  
http://dl2.pro.antivir.de/upd
```

При выполнении обновлений через файловый сервер (общая папка), введите UNC путь к общей папке:

```
\\<server>|<IP address>\<share>\<path>
```

#### – Update interval in minutes

Введите интервал обновления в минутах. AntiVir SharePoint будет через установленные промежутки времени проверять доступность обновлений на указанном сервере и при необходимости запустит процесс обновления. Значение по умолчанию равно 120 минутам.

#### – Network user name

Введите имя пользователя для аутентификации, если для обновлений Вы используете общую папку на файловом сервере.

#### – Network password

Введите пароль для аутентификации, если для обновлений Вы используете общую папку на файловом сервере.

#### – Confirm network password

Подтвердите пароль.

### Proxy settings (настройки прокси)

Здесь указываются настройки сервера проху, если для обновления через web-сервер используется сервер проху.

– **Use of a proxy server**

Если активировать данную опцию, то AntiVir SharePoint будет соединяться с web-сервером обновлений через сервер прокси. Данная опция по умолчанию отключена.

– **Proxy URL**

Введите адрес URL или адрес IP проху-сервера.

– **Proxy port**

Введите номер порта проху-сервера.

– **Proxy user name**

Введите имя входа на проху-сервер.

– **Proxy password**

Введите пароль для входа на проху-сервер.

– **Confirm proxy password**

Подтвердите пароль.

### Settings for email notifications (настройки уведомлений по электронной почте)

Настройки уведомлений по электронной почте по протоколу SMTP. Вы можете получать уведомления либо при каждом обновлении, либо в случае неудачного обновления. Письмо с уведомлением содержит следующую информацию:

- Имя компьютера с AntiVir SharePoint
- Дата и время обновления
- Статус обновления
- Текущие версии обновленных файлов



Аутентификация пользователя на сервере SMTP не поддерживается.

---

---

– **Enable email notification**

При включенной опции отправляет уведомление по электронной почте.  
Данная опция по умолчанию выключена.

– **SMTP host name**

Введите имя сервера SMTP, который будет использоваться для рассылки уведомлений по электронной почте.

– **Event selection**

Выберите событие, о котором Вы должны быть уведомлены:

**Email sent for every update**

При каждом обновлении будет выслано уведомление (если файлы были обновлены).

**Email sent for defective update**

Уведомление будет выслано при некорректном обновлении.

– **SMTP sender name**

Введите имя или электронный адрес отправителя уведомления.

– **SMTP recipient name**

Введите адрес электронной почты получателя уведомления. Можно вводить несколько адресов, разделяя их запятыми.

## 9 Обновления

Эффективность антивирусной защиты зависит полностью от актуальности антивирусных баз и ядра программы. Поэтому мы рекомендуем регулярно обновляться с наших серверов в Интернете. Служба обновлений обновляет следующие компоненты:

- Virus definition file (файл вирусных сигнатур)
- Scanning engine (ядро программы)

В AntiVir Administration в подменю update configuration создайте задачи обновлений, которые будут выполняться в запланированные интервалы времени службой обновлений Update service. Во время выполнения каждой задачи обновлений сравниваются версии файлов и, при необходимости, выполняется обновление. Обновление можно стартовать вручную через AntiVir Administration закладка **Status :: Last update**. После обновления нет необходимости перезапускать AntiVir

SharePoint. Обновления можно получить со следующих серверов:

- напрямую из Интернета через web-сервер Avira GmbH. Доступны следующие сервера обновлений:  
<http://dl1.pro.antivir.de/upd>  
<http://dl2.pro.antivir.de/upd>  
<http://dl3.pro.antivir.de/upd>  
<http://dl1.antivir.net/upd>  
<http://dl2.antivir.net/upd>  
<http://dl3.antivir.net/upd>
- через web-сервер или файловый сервер в локальной сети, который скачивает обновления из Интернета и раздает их компьютерам в сети. Это полезно, если Вы собираетесь обновлять больше одного компьютера в сети. Такой способ обновления позволяет поддерживать антивирусную защиту в актуальном состоянии и при этом экономить ресурсы.

При использовании web-сервера загрузка происходит по протоколу HTTP. При использовании файлового сервера доступ к файлам обновлений происходит по сети.



Вы можете использовать AntiVir Internet Update Manager (файловый или web-сервер под Windows) или AntiVir Mirror Script (файловый сервер под Linux) в качестве web-сервера или файлового сервера в локальной сети. Эти программы делают локальные зеркала серверов обновлений продуктов AntiVir (например, AntiVir SharePoint) и доступны для скачивания в Internet по адресу <http://www.avira.com>.

## 10 Информация и сервис

### 10.1.1 Подозрительные файлы

Вы можете отослать вирусы, которые не определяются или не удаляются продуктами AntiVir.

Отшлите файлы в виде архива (WinZIP, PKZip, Arj и т.д.) по адресу [virus@avira.com](mailto:virus@avira.com). Так как многие почтовые сервера защищены антивирусным ПО, рекомендуется файл архива защитить паролем (не забудьте указать пароль).

Также можно отослать подозрительные файлы через наш сайт.

### 10.1.2 Ложные срабатывания

Если Вы считаете, что AntiVir сработал на "чистый" файл, пожалуйста, пришлите нам заархивированный файл по адресу [virus@avira.com](mailto:virus@avira.com). со ссылкой, что это ложное срабатывание. Обязательно защитите архив при помощи пароля.



**Представительство Avira GmbH  
в России и Украине  
ООО "Антивирус-Центр" (Россия)**

308000, Россия,  
г. Белгород, пр-т. Богдана Хмельницкого 26/2  
Телефон:  
(4722) 353 - 701 (многоканальный)  
(4722) 329 - 688 (факс)  
<http://www.avirus.ru>

e-mail:  
[info@avirus.ru](mailto:info@avirus.ru) - Общая информация  
[marketing@avirus.ru](mailto:marketing@avirus.ru) - Отдел по работе с Партнерской Сетью  
[support@avirus.ru](mailto:support@avirus.ru) - Отдел технической поддержки

© Avira GmbH. All rights reserved.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH.

Errors and technical subject to change.

Issued Q4/2007

AntiVir® is a registered trademark of the Avira GmbH.

All other brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.