3.3	1. Антивирусное программное обеспечение. 2. Резервное копирование. Создание образа системы.			2	Выполнение практических заданий

1. Антивирусное программное обеспечение

Краткие теоретические сведения:

1) Введение

Антивирусное программное обеспечение – специализированная программа (или набор программ) для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Антивирусные программы подразделяются по признаку размещения в оперативной памяти на:

резидентные (начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов);

нерезидентные (запускаются по требованию пользователя или в соответствии с заданным для них расписанием).

Наиболее надежными в плане защиты от вирусов обычно считаются резидентные программы, использующие современные технологии комплексного анализа, выявления и деактивации вредоносных файлов и их последствий (наиболее распространенными являются: Norton AntiVirus, Doctor Web, Kaspersky Antivirus, AVG, Avast Free Antivirus, McAfee Total Protection, Comodo Antivirus и др.). Указанные антивирусы способны эффективно сканировать оперативную память и носители информации (внутренние и внешние), блокировать действие вирусов и осуществлять «лечение» зараженных файлов.

Однако, такие программы практически бессильны в ситуации, когда их установка либо функционирование оказываются невозможной в результате действий неизвестных ранее вирусов или по какой-либо другой причине (например, в результате несвоевременного обновления антивирусных баз, некорректного использования списка исключений, использования бесплатной антивирусной программы с ограниченными возможностями и др.).

Кроме того, какой бы эффективной не была бы антивирусная программа, она не в состоянии гарантировать 100%-ную защиту от вредоносных файлов. В случае заражения компьютера вирусами и невозможности использования встроенных программных средств защиты альтернативным способом восстановления его работы может быть использование нерезидентных антивирусных программных средств. К одной из таких программ относится бесплатная лечащая утилита Dr.Web CureIt. Она представляет собой

антивирусный сканер на основе стандартного сканирующего ядра продуктов семейства Dr.Web. Несмотря на некоторые ограничения по сравнению с антивирусом Dr.Web для Windows (отсутствие резидентного монитора, консольного сканера и модуля автоматического обновления и так далее), Dr.Web CureIt способен эффективно проверять систему и выполнять необходимые действия для обезвреживания обнаруженных угроз (утилита обнаруживает и обезвреживает следующие типы вредоносных программ: черви; вирусы; трояны; руткиты; шпионские программы; программы дозвона; рекламные программы; программы взлома; потенциально опасные программы).

Утилита Dr.Web CureIt, имеющая в своем составе самые последние вирусные базы Dr.Web, доступна для скачивания по адресу: https://free.drweb.ru/cureit/. При этом, поставляемый в ее набор вирусных баз актуален только до выхода нового дополнения (как правило, дополнения выпускаются один или несколько раз в час). Поэтому для осуществления антивирусной проверки данную утилиту следует скачивать с указанного сайта каждый раз заново.

2) Запуск Dr.Web CureIt. Быстрая антивирусная проверка

Рассмотрим алгоритм действий по использованию предустановленного шаблона быстрой проверки наиболее уязвимых объектов операционной системы инфицированного ПК с помощью утилиты Dr.Web CureIt.

1. Используя «чистый» компьютер, скачайте с официального сайта утилиту Dr.Web CureIt, сохранив ее на USB-носитель (желательно, с последующей установкой защиты от записи).
2. Вставьте USB-носитель в инфицированный ПК и запустите сохраненный файл на исполнение (дважды щелкните по нему левой кнопкой мышки).
3. В первом окне «Лицензия и обновление» ознакомьтесь с условиями отправки статистики. Нажмите кнопку *Продолжить*.
4. В окне выбора типа проверки нажмите кнопку *Начать проверку* (рис. 1). В этом режиме утилита Dr.Web CureIt использует предустановленный шаблон быстрой проверки наиболее уязвимых объектов операционной системы

В данном режиме производится проверка следующих объектов:

оперативная память;
загрузочные секторы всех дисков;
корневой каталог загрузочного диска;
корневой каталог диска установки Windows;
системный каталог *Windows*;
папка *Мои Документы*;
временный каталог системы;
временный каталог пользователя;
наличие руткитов.

Рис. 1. Запуск утилиты Dr.Web CureIt для быстрой антивирусной провреки

В процессе проверки в окне отображается общая информация о ее ходе, а также список обнаруженных угроз (рис. 2).

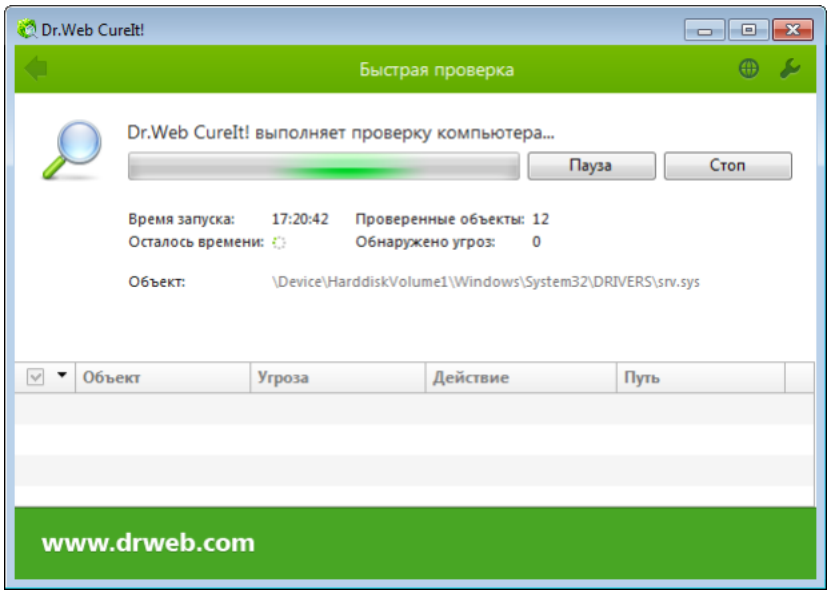


Рис. 2. Общая информация о ходе проверки, а также список обнаруженных угроз

5. По завершении проверки информация об обнаруженных угрозах приводится в окне отчета. При необходимости вы можете просмотреть файл отчета о проверке. Для этого нажмите кнопку *Открыть отчет*.

6. Если в ходе проверки были обнаружены вирусы или угрозы других типов, их необходимо нейтрализовать. Чтобы применить предустановленные действия, нажмите кнопку *Обезвредить* (рис. 3). При необходимости вы можете настроить разные действия для конкретных угроз.

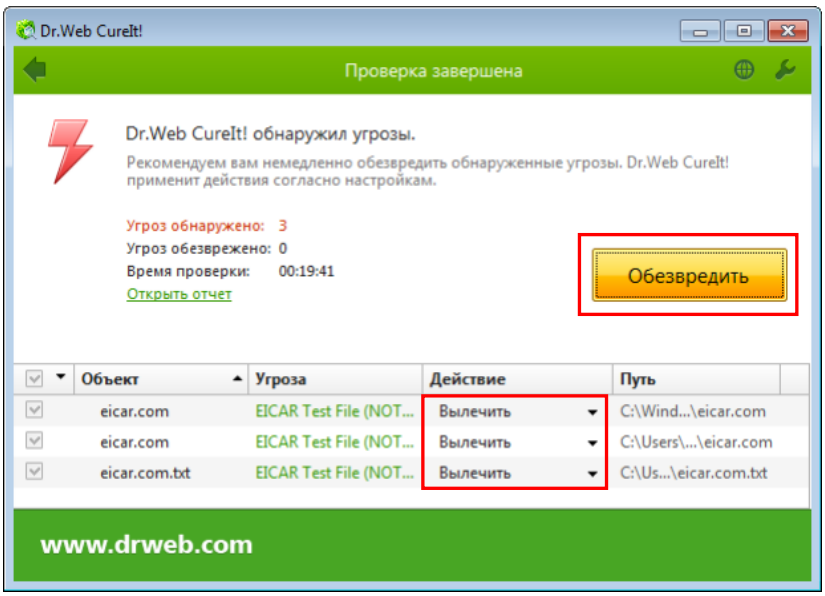


Рис. 3 Нейтрализация выявленных угроз утилитой Dr.Web CureIt

По окончании проверки Dr.Web CureIt лишь информирует об обнаруженных угрозах и предлагает применить к ним наиболее оптимальные действия по обезвреживанию. При необходимости вы можете вручную выбрать конкретные объекты или группы объектов, для которых по нажатию кнопки *Обезвредить* требуется применить действия. Для этого используйте флажки рядом с названиями объектов или выпадающее меню в заголовке таблицы.

Вы также можете применить действие для каждой угрозы по отдельности. Вы можете восстановить функциональность зараженного объекта (вылечить его), а при невозможности – устранить исходящую от него угрозу (удалить объект).

В большинстве случаев для полного излечения компьютера от заражения достаточно провести быструю проверку. В случаях, когда необходима тонкая настройка процедуры проверки, вы можете воспользоваться следующими дополнительными возможностями:

проведение выборочной проверки, в ходе которой можно указать конкретные объекты операционной системы и отдельные папки и файлы для проверки;

выбор действий по обезвреживанию обнаруженных угроз;

общая настройка параметров антивирусной проверки;

запуск утилиты Dr.Web CureIt с параметрами командной строки.

3) Выборочная антивирусная проверка

Для того, чтобы осуществить выборочную проверку ПК, необходимо выполнить следующую последовательность действий:

1. При запуске утилиты окне выбора типа проверки нажмите на ссылку «*Выбрать объекты для проверки*» (рис. 4).

Рис. 4. Запуск выборочной антивирусной проверки с помощью утилиты Dr.Web CureIt

2. В открывшейся таблице в центре окна «Выборочная проверка» выберите объекты для проверки (рис. 5). Чтобы добавить в список конкретный файл или папку, щелкните по ссылке в нижней части поля таблицы и выберите нужный объект в окне *Обзор*.

Чтобы выбрать все указанные в таблице объекты, установите флажок *Объекты проверки* в заголовке таблицы.

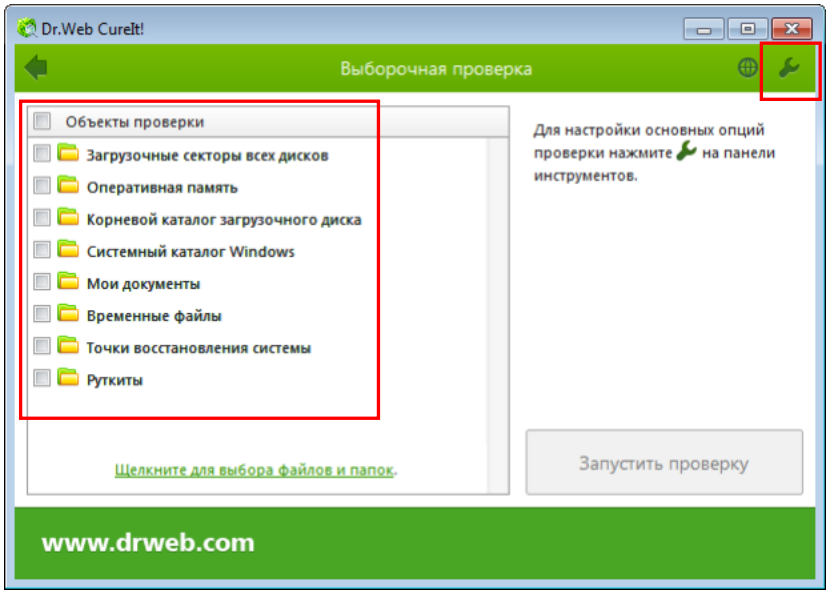


Рис. 5. Окно настройки выборочной антивирусной проверки с помощью утилиты Dr.Web CureIt

4) Настройка параметров работы Dr.Web CureIt

При необходимости перед началом проверки настройте параметры работы Dr.Web CureIt. Для этого на панели инструментов нажмите кнопку *Параметры проверки*.

Откроется окно настроек, содержащее следующие вкладки (рис. 6):

Основные, в которой задаются общие параметры работы утииты;

Действия, в которой задается реакция утилиты на обнаружение зараженных или подозрительных файлов и вредоносных программ;

Исключения, в которой задаются дополнительные ограничения на состав файлов, подлежащих проверке;

Отчет, в которой задается режим ведения файла отчета о проверке.

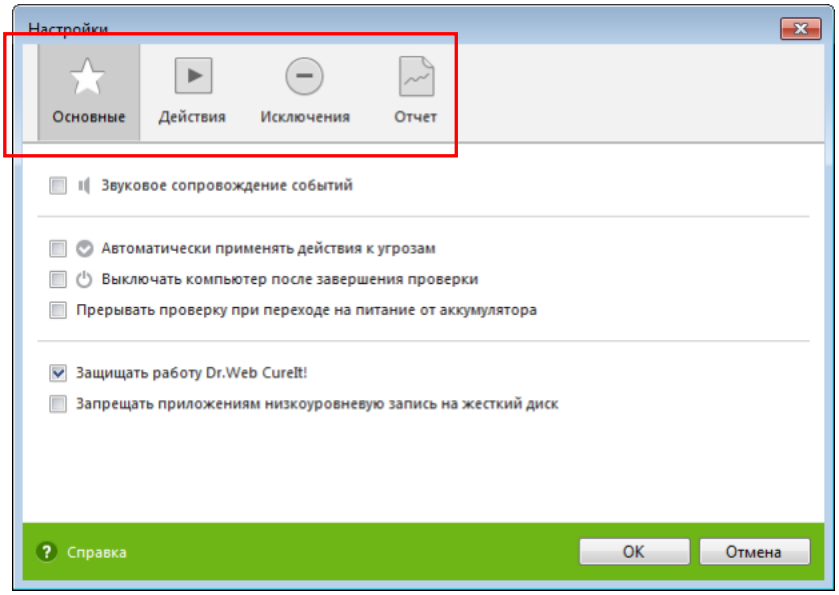


Рис. 6. Окно настройки параметров работы утилиты Dr.Web CureIt

Рассмотрим основные настройки утилиты более подробно.

На вкладке *Основные* (рис. 6) вы можете включить звуковое сопровождение событий, настроить взаимодействие программы с операционной системой, а также указать Dr.Web CureIt автоматически применять действия к угрозам. В данном разделе вы также можете настроить параметры самозащиты, а также запретить некоторые действия, которые могут привести к заражению вашего компьютера.

На вкладке *Действия* можно настроить оптимальные действия по обезвреживанию обнаруженных угроз (рис. 7).

Оптимальной реакцией на обнаружение излечимых угроз (например, зараженных вирусами файлов) является лечение, в ходе которого восстанавливается исходное состояние объекта, имевшееся до заражения. Угрозы других типов рекомендуется перемещать в карантин, что позволяет предотвратить случайную потерю ценных данных.

Перечень возможных устанавливаемых реакций на обнаружение угроз представлен в таблице 1.

При обнаружении вирусов или подозрительного кода внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров) действия по отношению к угрозам внутри таких объектов выполняются над всем объектом, а не только над зараженной его частью. По умолчанию во всех этих случаях предусмотрено перемещение объекта в карантин.

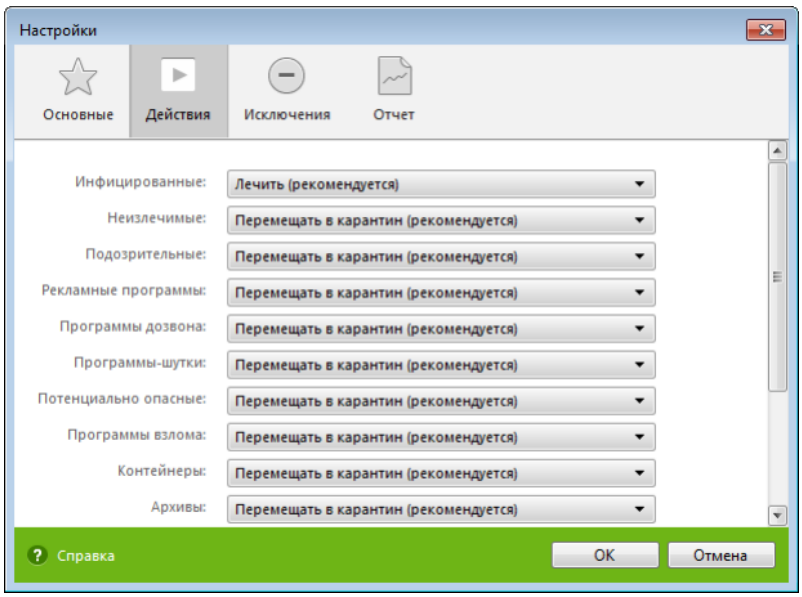


Рис. 7. Окно настройки параметров «Действия» утилиты Dr.Web CureIt

Таблица 1

Перечень возможных реакций на обнаружение угроз

Действие	Описание
Лечить	Восстановить состояние объекта, имевшееся до заражения. Если вирус неизлечим или попытка лечения не была успешной, будет выполнено действие, заданное для неизлечимых объектов. Лечение возможно только для объектов, зараженных известным излечимым вирусом, за исключением троянских программ и зараженных файлов внутри составных объектов (архивов, файлов электронной почты или файловых контейнеров). Троянские программы при обнаружении удаляются. Лечение – это единственное действие, доступное для зараженных загрузочных секторов.
Перемещать в карантин	Переместить объект в специальную папку для изоляции. По умолчанию карантин расположен в скрытой папке %USERPROFILE%\Doctor Web\CureIt Quarantine\ и становится доступен после окончания проверки. Для загрузочных секторов никаких действий производиться не будет.
Удалять	Полностью удалить объект из системы. Для загрузочных секторов никаких действий производиться не будет.
Игнорировать	Пропустить объект без выполнения каких-либо действий и не выводить информацию в отчете. Данное действие возможно только для вредоносных программ: рекламные программы, программы дозвона, программы-шутки, потенциально опасные программы и программы взлома.

Для успешного завершения лечения некоторых зараженных (инфицированных) файлов требуется перезагрузка операционной системы. Вы можете выбрать один из вариантов:

предлагать перезагрузку;

перезагружать компьютер автоматически. Этот режим может привести к потере несохраненных данных.

На вкладке *Исключения* (рис. 8) задается дополнительное ограничение на состав файлов, которые должны быть подвергнуты проверке в соответствии с заданием на сканирование, а также указывается, требуется ли проводить проверку содержимого архивов и инсталляционных пакетов.

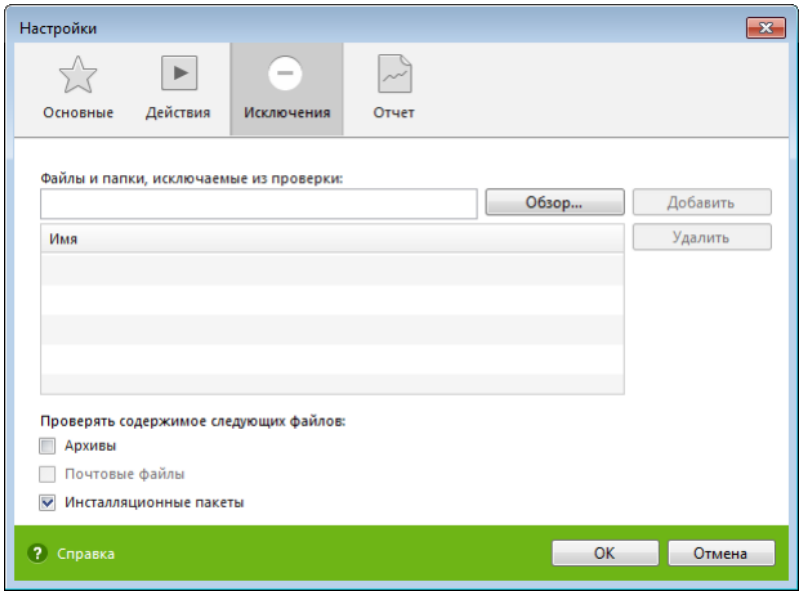


Рис. 8. Окно настройки параметров «Исключения» утилиты Dr.Web CureIt

Здесь можно задать список файлов (масок файлов), которые не будут сканироваться (из проверки будут исключены все файлы с данным именем). В таком качестве могут выступать временные файлы (файлы подкачки) и т. п.

Чтобы задать список исключаемых файлов, выполните одно из следующих действий:

1) Введите имя (маску) файла, который должен быть исключен из проверки. Если вводится имя существующего файла, можно воспользоваться кнопкой *Обзор* и выбрать объект в стандартном окне открытия файла. Также вы можете использовать маски.

Маска задает общую часть имени объекта:

символ «*» заменяет любую, возможно пустую последовательность символов;

символ «?» заменяет любой, но только один символ;

остальные символы маски ничего не заменяют и означают, что на этом месте в имени должен находиться именно этот символ.

Примеры:

отчет.doc* – маска, задающая все документы Microsoft Word, название которых начинается с подстроки «отчет», например, файлы отчет-февраль.doc, отчет121209.doc и т. д.;

**.exe* – маска, задающая все исполняемые файлы с расширением EXE, например, setup.exe, iTunes.exe и т. д.;

photo????09.jpg – маска, задающая все файлы изображений формата JPG, название которых начинается с подстроки «photo» и заканчивается подстрокой «09», при этом между двумя этими подстроками в названии файла стоит ровно четыре произвольных символа, например: *photo121209.jpg, photomama09.jpg* или *photo----09.jpg*.

2) Нажмите кнопку *Добавить*, расположенную справа. Файл (маска файла) будет добавлен в список, расположенный ниже.

Чтобы удалить какой-либо объект из списка, выберите его в списке и нажмите кнопку *Удалить*. Файл будет допущен к последующей проверке.

На вкладке *Отчет* (рис. 9) задается режим ведения файла отчета.

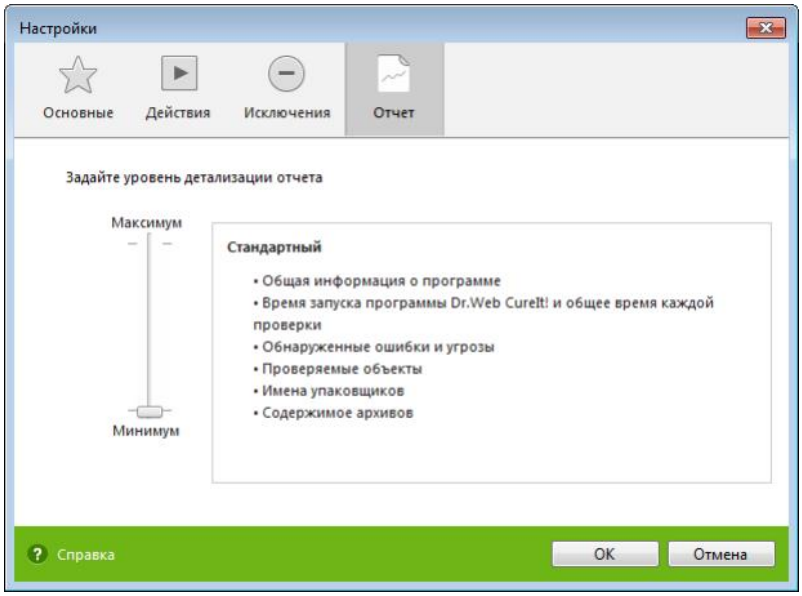


Рис. 9. Окно настройки параметров «Отчет» утилиты Dr.Web CureIt

Вы можете задать одну из следующих степеней детальности ведения отчета:

Стандартный – в данном режиме в отчете фиксируются только наиболее значимые события, такие как запуск и остановка Dr.Web CureIt и обнаруженные угрозы;

Отладочный – в данном режиме в отчете фиксируется максимальное количество информации о работе Dr.Web CureIt, что может привести к значительному увеличению файла отчета. Рекомендуется использовать этот режим только при возникновении проблем в работе Dr.Web CureIt или по просьбе технической поддержки компании «Доктор Веб».

Подробный отчет о работе Dr.Web CureIt хранится в файле CureIt.log, расположенном в каталоге %USERPROFILE%\Doctor Web. Рекомендуется периодически анализировать файл отчета.

По окончании редактирования настроек нажмите кнопку *Ок* для сохранения внесенных изменений или кнопку *Отмена* для отказа от них.

Изменение настроек имеет силу только в данном сеансе работы Dr.Web CureIt. При повторном запуске утилиты все настройки автоматически возвращаются к первоначальным значениям.

4. Нажмите кнопку *Запустить проверку*.

По завершении проверки информация об обнаруженных угрозах приводится в окне отчета.

5) Менеджер карантина

Для изоляции файлов с потенциальными угрозами в программе Dr.Web CureIt предусмотрен *менеджер карантина*. Каталог карантина находится по локальному адресу: *%USERPROFILE%\DoctorWeb\CureItQuarantine*. Файлы с угрозами, найденные на несъемных дисках, шифруются. Для открытия соответствующего окна программы следует нажать на *Параметры проверки* и выбрать *Менеджер Карантина*. В окне отображена таблица со следующими полями: Объект – имена файлов, расположенных в карантине (рис. 10).

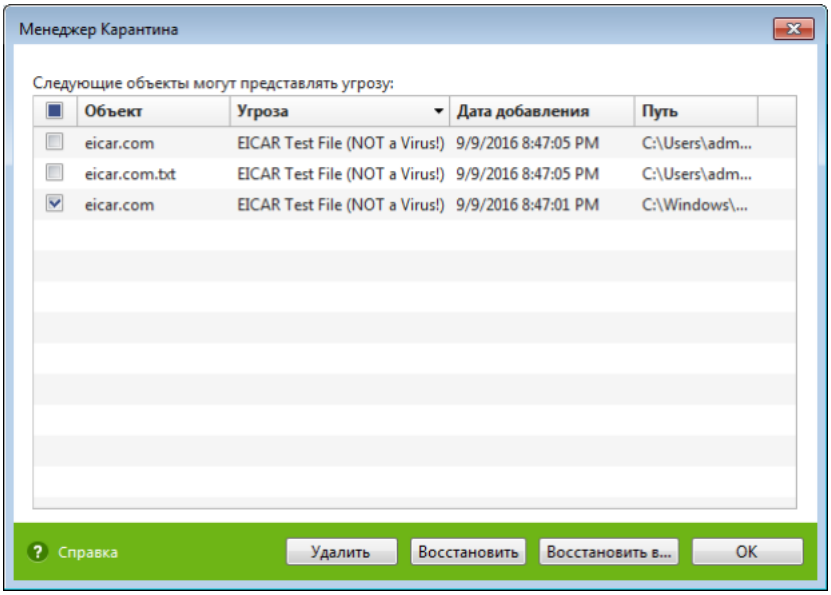


Рис. 10. Окно настройки параметров «Менеджер Карантина» утилиты Dr.Web CureIt

В центральной части окна отображается таблица с информацией о состоянии Карантина, включающая следующие поля:

объект – имя объекта, находящегося в карантине;

угроза – классификация вредоносной программы, определяемая Dr.Web CureIt при автоматическом перемещении объекта в карантин;

дата добавления – дата, когда объект был перемещен в карантин;

путь – полный путь, по которому находился объект до перемещения в карантин.

В окне *Менеджер Карантина* файлы могут видеть только те пользователи, которые имеют к ним доступ.

Чтобы отобразить скрытые объекты, запустите Dr.Web CureIt под административной учетной записью.

В окне *Менеджер Карантина* доступны следующие кнопки управления:

Восстановить – переместить файл из карантина и восстановить первоначальное местоположение файла на компьютере (восстановить файл под тем же именем и в папку, в которой он находился до перемещения в карантин).

Восстановить в – переместить файл под заданным именем в нужную папку.

Используйте данную функцию только в том случае, если вы уверены, что объект безопасен.

Удалить – удалить файл из карантина и из системы.

Для одновременной работы с несколькими файлами установите флажки рядом с названиями объектов, а затем выберите необходимое действие.

6) Проверка антивирусного программного обеспечения

Вы можете проверить работоспособность антивирусных программ, обнаруживающих вирусы по их сигнатурам, с использованием тестового файла EICAR – European Institute for Computer Anti-Virus Research.

Многими разработчиками антивирусов принято для этой цели использовать одну и ту же стандартную программу *test.com*. Эта программа была специально разработана для того, чтобы пользователь, не подвергая свой компьютер опасности, мог посмотреть, как установленный антивирус будет сигнализировать об обнаружении вируса. Программа test.com не является сама по себе вредоносной, но специально обрабатывается большинством антивирусных программ как вирус (рис. 11). Dr.Web CureIt называет этот «вирус» следующим образом: *EICAR Test File (Not a Virus!)*. Примерно так его называют и другие антивирусные программы.

Программа *test.com* представляет собой 68-байтный COM-файл, в результате исполнения которого на консоль выводится текстовое сообщение *EICAR-STANDARD-ANTIVIRUS-TEST-FILE!*

Файл test.com состоит только из текстовых символов, которые формируют строку:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Если вы создадите файл, содержащий приведенную выше строку, и сохраните его под именем *test.com*, то в результате получится программа, которая и будет описанным «вирусом».

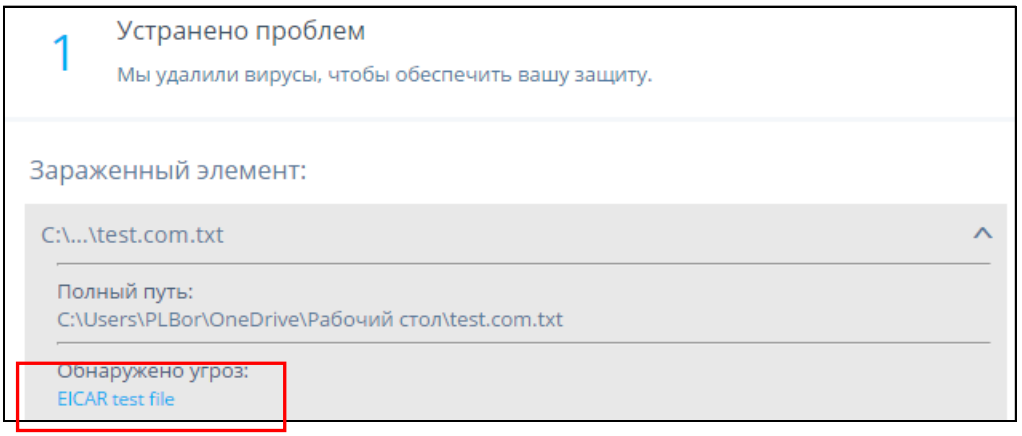


Рис. 11. Программа test.com обрабатывается большинством антивирусных программ как вирус

8) Онлайн-анализ подозрительных файлов и ссылок (URL) на предмет выявления вредоносного программного обеспечения

Одним из распространенных способов заражения вирусами является открытие вредоносных ссылок (URL) на веб-сайтах, новостных лентах и социальных сетях. Злоумышленники прибегают к самым различным уловкам: размещают вредоносные ссылки на перегруженной информацией странице, надеясь наткнуться на тех, кто нажимают на ссылки без разбора, взламывают учетные записи и отправляют ссылки друзьям из списка контактов, полагая что такому источнику автоматически проявят доверие, они также подделывают URL так, чтобы казалось, что ссылка ведет к другой, заведомо законопослушной странице.

Особую значимость рассматриваемая проблема приобрела с распространением онлайн-сервиса «Bit.ly» (https://bitly.com), предназначенного для создания сокращенных URL. Этот сервис сокращает ссылку, превращая её фактически в семь символов, следующих за приставкой-названием самого сервиса, например: *bit.ly/2ByeRZX*. Суть такого сокращения – сделать ссылку более компактной для рассылки через E-mail, уведомления и SMS, а следовательно – более кликабельной.

Однако, короткие ссылки существенно упрощают злоумышленнику работу, поскольку они позволяют скрыть, куда на самом деле производится переход. Так, в почту, на страницу социальной сети либо на мобильные устройства обычных пользователей зачастую приходят различные SMS-сообщения со ссылкой на сайт Bit.ly. Содержание таких посланий может быть самым разным, например: «*Посмотри фото bit.ly/2zobpB6*», либо «*Вам одобрен займ bit.ly/creditplus*». При переходе по такой ссылке на устройство загружается файл, который пользователь принимает за обещанное фото либо иные материалы. При его открытии запускается установка вредоносной программы («троян», «червь», кейлоггер и т. п.), которая действует по заранее предопределенному злоумышленником алгоритму: загружает рекламные приложения, перехватывает личные данные, оформляет платные подписки на онлайн-сервисы, сканирует систему на наличие банковских приложений и кошельков, осуществляет взлом мобильного банкинга и пр.

Сайты, которые могут нанести урон информационной безопасности пользовательского устройства, делятся на две основные категории:

сайты с вредоносным ПО, которые устанавливают на устройство пользователя программы, которые позволяют злоумышленникам выполнять различные несанкционированные действия, например получать личную информацию;

фишинговые сайты, которые внешне выглядят как обычные веб-ресурсы и пытаются убедить пользователя ввести учетные данные или другие конфиденциальные сведения. Чаще всего они выдают себя за официальные сайты банков или интернет-магазинов.

Для того, чтобы проверить подозрительный файл либо ссылку (URL) на предмет выявления вредоносного программного обеспечения, не открывая их,

рекомендуется воспользоваться одним из онлайн-сервисов, например: VirusTotal (https://www.virustotal.com/) (рис. 12).

Рис. 12. Онлайн-сервис для анализа подозрительных файлов и ссылок (URL) на предмет выявления вредоносного программного обеспечения (virustotal.com)

Отличительной особенностью данного онлайн-сервиса является то, что он использует данные 57 различных антивирусных баз (Avira, Comodo Site Inspector, Dr.Web, Google Safebrowsing, Kaspersky, ESET, Netcraft и др.).

Для того, чтобы проверить на вирусы ссылку (например, *http://bit.ly/1dNVPAW*), ее следует скопировать в буфер обмена, нажать на вкладку *URL* данного сервиса, затем вставить из буфера обмена эту ссылку в специальное поле для ввода и нажать клавишу *Enter*.

Пример диалогового окна с результатами антивирусной проверки указанной ссылки представлен на рис. 13.

Результаты анализа позволяют сделать вывод, что исследуемая ссылка (URL) с определенной долей вероятности ссылается на вредоносную программу типа *Malware*. К примерам явных вредоносов *Malware* можно отнести рекламные и им подобные программы. К их признакам относятся следующие:

изменение настроек браузера (изменение стартовой страницы браузера, стандартной страницы поиска, несанкционированное открытие новых окон, ведущих на определенные сайты и т.п.), если восстановленные настройки снова меняются после перезагрузки компьютера. Такое изменение является признаком проникновения рекламной или троянской программы, которая направляет пользователя на сайт, содержащий *Malware*;

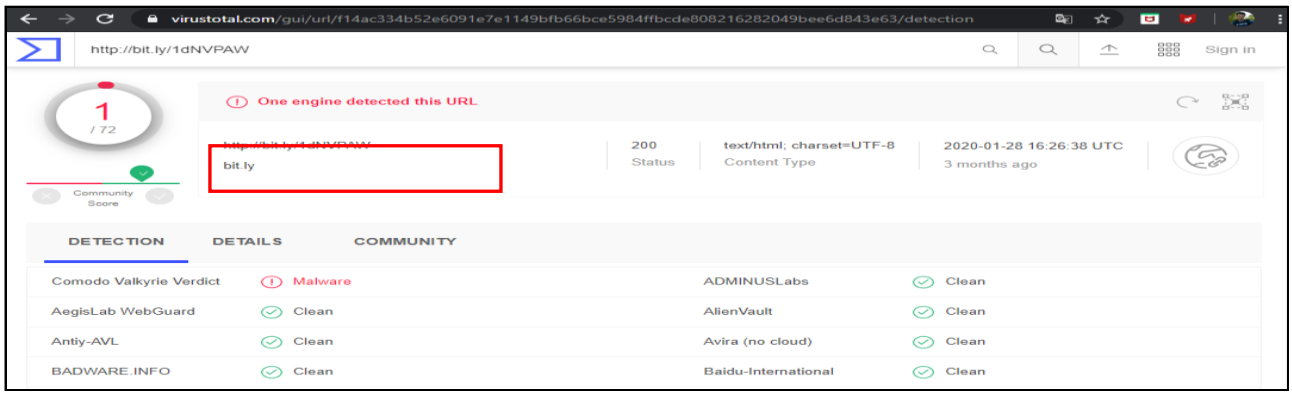


Рис. 13. Онлайн-сервис для анализа подозрительных файлов и ссылок (URL) на предмет выявления вредоносного программного обеспечения (virustotal.com)

всплывающие и другие сообщения, похожие на стандартные служебные сообщения операционной системы и содержащие гиперссылки или кнопки для перехода на замаскированный вредоносный сайт;

получение множества системных сообщений об ошибке;

пропажа или несанкционированное изменение файлов или папок;

компьютер часто зависает, или программы стали выполняться медленно.

Признаками проявлений косвенных *Malware* могут быть следующие:

блокирование антивируса: многие Malware пытаются выгрузить антивирус из памяти или даже удалить файлы антивируса с дисков компьютера;

блокирование антивирусных сайтов: другие *Malware* нейтрализуют только возможность обновления антивирусных средств, т.е. не блокируют доступ в Интернет целиком, а только доступ к сайтам и серверам обновлений наиболее известных производителей антивирусов;

сбои в системе или в работе других программ, что проявляется появлением сообщений о необычных ошибках;

происходит неожиданный запуск программ (загорается индикатор доступа к жесткому диску, хотя пользователь не запускал никаких программ);

при включении компьютера операционная система не загружается.

Для того, чтобы проверить файл, который находится на вашем устройстве либо внешнем носителе, необходимо на вкладке *File* нажать на кнопку *Choose file*, указать путь к файлу и нажать *Check file* (рис. 14).

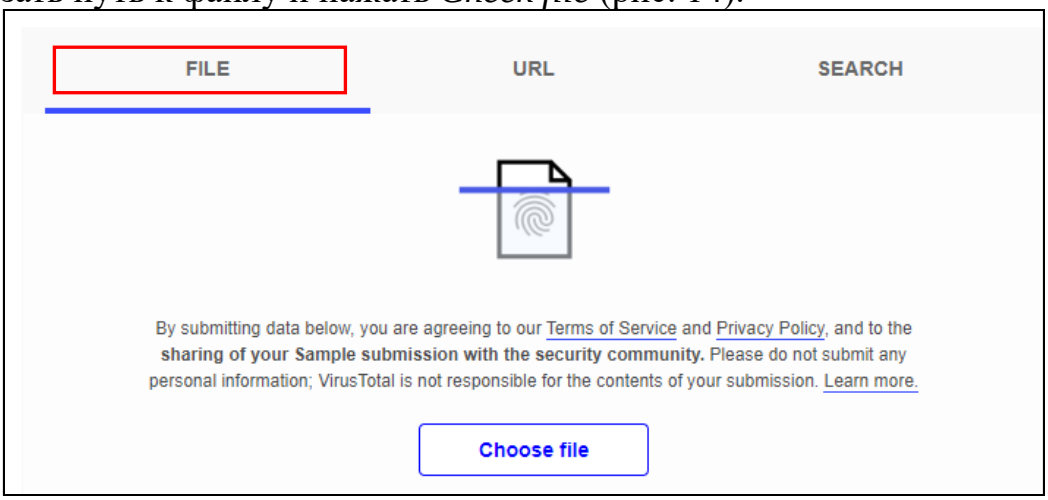


Рис. 14. Онлайн-сервис для анализа подозрительных файлов и ссылок (URL) на предмет выявления вредоносного программного обеспечения (virustotal.com)

Результаты проверки подозрительного файла с помощью онлайн-сервиса VirusTotal представлены на рис. 15.

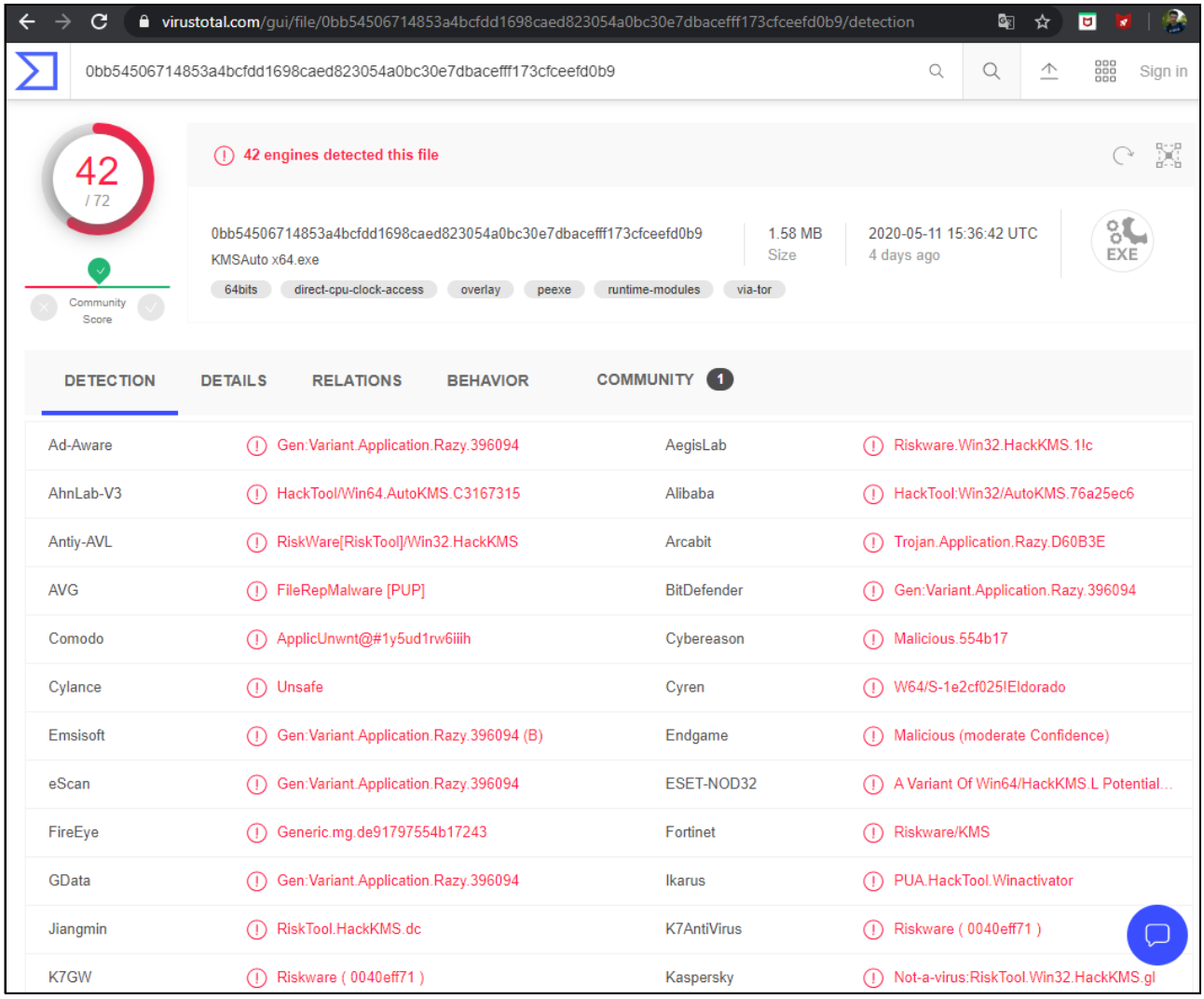


Рис. 15. Результаты проверки подозрительного файла с помощью онлайн-сервиса VirusTotal.

Все проверяемые файлы заносятся в общую базу, поэтому возможна ситуация, когда файл уже проверялся. В этом случае на экран будет выдано уведомление и можно либо посмотреть результаты предыдущей проверки, либо проверить заново.

Существует также альтернативные онлайн-сервисы анализа подозрительных ссылок (URL) на предмет выявления вредоносного программного обеспечения.

Так, онлайн-сервис CheckShortURL (http://checkshorturl.com/) предназначен для проверки коротких (сокращенных) ссылок, создаваемых большинством сервисов сокращения URL (рис. 17). Введите короткий адрес, и CheckShortURL проведет анализ и сообщит, куда ведет ссылка. Сервис позволяет сделать предварительный просмотр сайта, чтобы убедиться в его благонадежности. В случае, если у пользователя возникнут сомнения по поводу безопасности сайта, то на CheckShortURL можно автоматически провести поиск

сайта в различный сервисах по оценке безопасности, например, таких как Web of Trust.

Рис. 17. Онлайн-сервис CheckShortURL (http://checkshorturl.com/) для проверки ссылок URL

В случае, когда необходимо установить, что именно происходит в процессе переадресации при нажатии на короткую ссылку, рекомендуется воспользоваться онлайн-сервисом GetLinkInfo (http://getlinkinfo.com/) (рис. 18). Данный сервис позволяет проследить, через какие этапы проходит переадресация. Для оценки безопасности GetLinkInfo использует технологии безопасного просмотра Google.

Рис. 18. Онлайн-сервис GetLinkInfo (http://getlinkinfo.com/) для проверки ссылок URL

Кроме того, на некоторых сервисах сокращения URL понимают, что есть смысл в предоставлении возможности пользователям заглянуть «за кулисы». Некоторые из них предлагают метод проверки сгенерированных на их сайте ссылок, чтобы пользователям не приходилось идти на риск. Например, если добавить «+» к концу ссылки Bit.ly, то пользователь перейдет на страницу

предварительного просмотра перед тем, как перейдет к самому файлу или сайту. Например: *http://bit.ly/1dNVPAW+*.

Для осуществления оперативного онлайн-анализа файлов и ссылок на мобильных устройствах рекомендуется воспользоваться специальным ботом[1] в мессенджере Telegram: @drwebbot (https://telegram.me/drwebbot) (рис. 19).

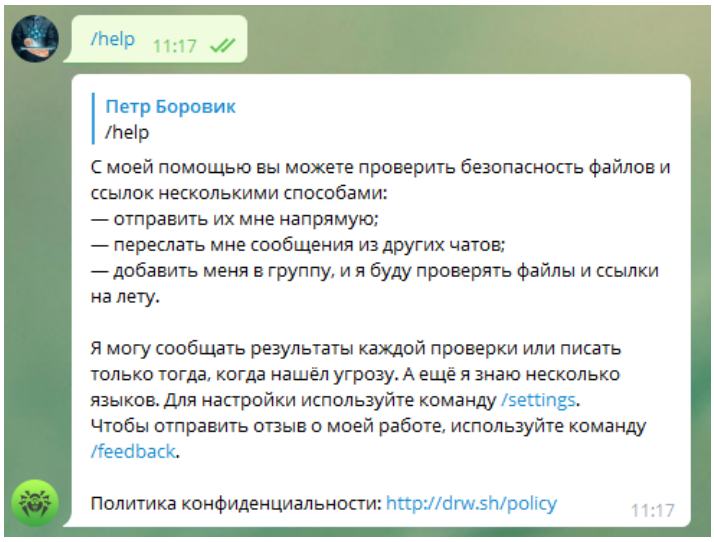


Рис. 19. Онлайн-сервис (бот) @drwebbot (https://telegram.me/drwebbot) для проверки ссылок URL на мобильном устройстве

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 3.2»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

1. Скачайте Dr.Web CureIt, сохранив утилиту на жесткий диск.

2. Запустите сохраненный файл на исполнение. Установите русский язык интерфейса. Осуществите настройку следующих параметров антивирусной проверки:

а) установите запрет приложениям на низкоуровневую запись на жесткий диск;

б) предусмотрите следующие действия при обнаружении вредоносных файлов: *инфицированные* – лечить; *неизлечимые* – удалять; *программы взлома* – удалять. Действия на остальные угрозы – перемещать в карантин;

---

[1] Бот – специальный аккаунт в Telegram, созданный для того, чтобы автоматически обрабатывать и отправлять сообщения. Пользователи могут взаимодействовать с ботами при помощи сообщений, отправляемых через обычные или групповые чаты.

в) включите проверку содержимого архивов;

г) выключите проверку инсталляционных пакетов;

д) задайте следующие объекты файловой системы, исключаемые из проверки: файлы, название которых начинается с подстроки «*diag*»; файлы с расширениями *txt, inf* и *jpg*; папки *C:\Program Files (x86)\Adobe*; *C:\Users\Public\Music; C:\Windows\Media.*

е) выберите следующие объекты для проверки: *загрузочные секторы всех дисков; системный каталог Windows; временный каталог системы; руткиты*.

3. Сохраните указанные настройки и осуществите проверку системы.

4. Дождитесь окончания сканирования и изучите содержимое отчета о проверке.

5. Откройте диалоговое окно *Менеджер карантина* и ознакомьтесь с его содержимым.

6. Используя полученную информацию, заполните в файле-отчете следующую таблицу:

Сведения о проведении антивирусной проверки	
Имя компьютера	
Дата проверки	
Общее время проверки	
Количество проверенных объектов	
Количество удаленных инфицированных объектов	
Количество инфицированных объектов, перемещенных на карантин	

7. На рабочем столе создайте папку *Подозрительные файлы*. Из сетевой папки, указанной преподавателем, скопируйте туда предложенные им файлы.

8. Откройте интернет-браузер и запустите онлайн-сервис VirusTotal (https://www.virustotal.com/). Проанализируйте с его помощью файлы, находящиеся в папке *Подозрительные файлы*.

Указанные файлы самостоятельно проанализируйте с помощью альтернативного онлайн-сервиса Kaspersky (https://opentip.kaspersky.com/?_ga=2.28098171.615941774.1594559580-1039091788.1594559580).

Сравните полученные результаты и зафиксируйте их в файле-отчете. Опишите вредоносные объекты (наименование проверенного объекта, название вируса, его прямые и косвенные признаки, возможные деструктивные действия и т. п.), находящиеся в указанных файлах. Сформулируйте выводы.

9. С помощью онлайн-сервиса VirusTotal проанализируйте следующие ссылки (URL):

https://rsincter.com/cro
http://nazar-chorniy.hol.es/
http://ty.esy.es
http://prazdniktost.tk/
bit.ly/1dNVPAW
bit.ly/1JcI49O

http://vk0ntakte.ru
https://VK0NTAKTE.RU
http://27sysday.ru/warning/ok/
https://all-link.agency/a56h/komsng/

Осуществите дополнительный анализ указанных ссылок с помощью альтернативных онлайн-сервисов анализа подозрительных ссылок (URL):

CheckShortURL (http://checkshorturl.com/),
GetLinkInfo (http://getlinkinfo.com/),
@drwebbot (https://telegram.me/drwebbot),
Kaspersky (https://opentip.kaspersky.com/?_ga=2.28098171.615941774.1594559580-1039091788.1594559580)

Результаты зафиксируйте в файле-отчете. Опишите вредоносные объекты (URL проверенной ссылки, название вируса либо угрозы, возможные деструктивные действия и т. п.). Сравните функциональные особенности использованных онлайн-сервисов. Сформулируйте выводы.

10. С помощью стандартной программы *Блокнот* создайте тестовый вирусный файл *test.com* (см. стр. 11) и сохраните его на рабочем столе.
11. Скачайте и установите десктопное приложение VirusTotal Uploader (https://www.virustotal.com/static/bin/vtuploader2.2.exe).
12. С помощью приложения VirusTotal Uploader проанализируйте файл *test.com*. Результаты зафиксируйте в файле-отчете.
13. С помощью приложения VirusTotal Uploader выявите и проанализируйте подозрительные системные процессы. При необходимости отправьте их на проверку. Результаты зафиксируйте в файле-отчете.
14. Осуществите запуск антивирусной утилиты Dr.Web CureIt из под командной строки со следующими параметрами:

а) сканировать все файлы в папке *Подозрительные файлы*;
б) проверять архивы;
в) сканировать файлы, на которые указывают ярлыки;
г) выполнять проверку загрузочных секторов и главных загрузочных секторов жесткого диска;
д) выполнять поиск угроз в оперативной памяти (включая системную область *Windows*);
е) сканировать системные точки восстановления;
ж) используя специальные модификаторы, настройте действия для различных угроз:

действия с инфицированными архивами – *вылечить;*
действия с неизлечимыми файлами – *удалить*;
действия с потенциально опасными файлами – *переместить в карантин;*
действия с подозрительными файлами – *игнорировать*.

Синтаксис команды запуска, а также результаты проверки зафиксируйте в файле-отчете.

15. Продемонстрируйте результаты преподавателю.

16. Подготовьте ответы на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

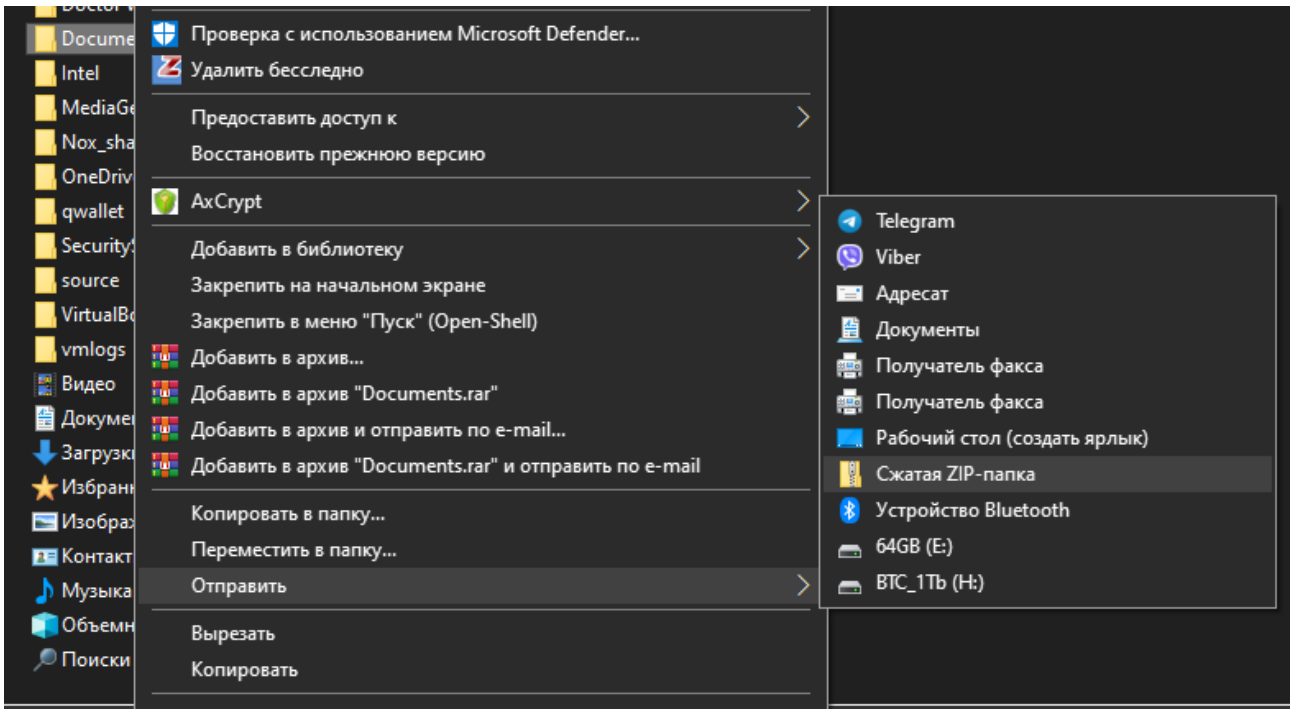
1. Опишите характерные черты компьютерных вирусов. Перечислите их деструктивные возможности. Перечислите основные (прямые и косвенные) признаки, свидетельствующие о заражении ПК вирусами
2. Какие методы лежат в основе механизма функционирования антивирусных программ? Перечислите виды антивирусных программ.
3. Опишите наиболее распространенные пути заражения компьютеров вирусами.
4. Основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
5. Какие объекты файловой системы ПК подлежат проверке в первую очередь при обнаружении признаков, свидетельствующих о заражении вирусами?
6. В чем состоят особенности и преимущества запуска антивирусной программы из-под командной строки?
7. Расскажите о перечне возможных устанавливаемых реакций антивирусной программы на обнаружение угроз.
8. Какой механизм предусмотрен в антивирусной программе для изоляции файлов с потенциальными угрозами?
9. Особенности использования сервисов онлайн-анализа подозрительных файлов и ссылок (URL) на предмет выявления вредоносного программного обеспечения. Приведите примеры.

2. Резервное копирование. Создание образа системы.

Краткие теоретические сведения:

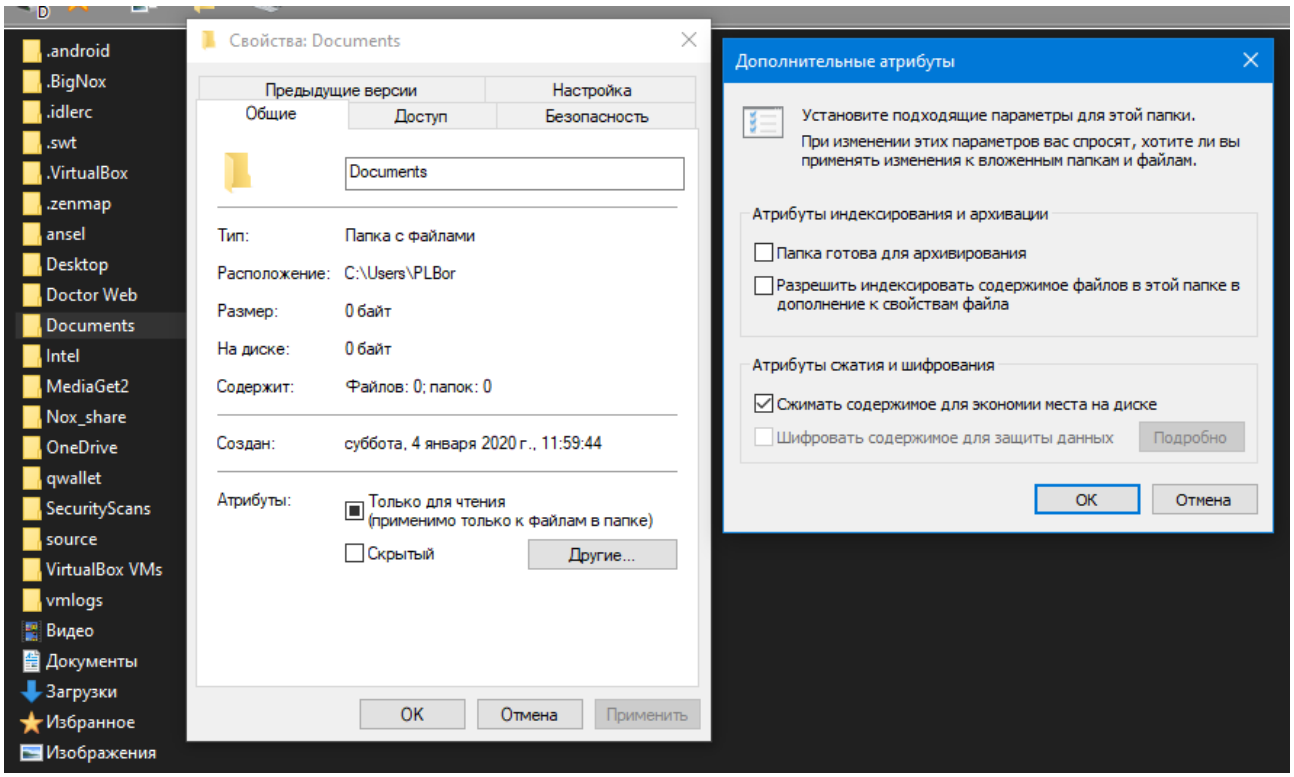
2.1. Резервное копирование файлов и папок в Windows путем предварительного сжатия и последующего копирования на другой носитель

Самый простой способ создать копию документа с важной информацией – просто скопировать файл на другой носитель. Например, на внешний жесткий диск. Заметим, что для уменьшения размера копируемой информации файлы можно предварительно сжать, создав архив с помощью какого-либо популярного архиватора, или воспользоваться встроенной возможностью самой операционной системы. Для этого выбираем файл, группу файлов или папку, “кликаем” правой клавишей мыши, в открывшемся меню выбираем пункт “Отправить” и в нем подпункт “Сжатая ZIP-папка”



Альтернативное решение использованию архиватора, создающего архивы сжатых файлов – использование функционала самой ОС Windows, позволяющего сэкономить дисковое пространство после определения носителя или отдельного каталога на таком носителе, как сжатого. Если выбираем для сжатия папку, размещенную на носителе с файловой системой NTFS, то в свойствах папки нажимаем кнопку “Другие”, в окне “Дополнительные атрибуты” устанавливаем флажок в чекбоксе “Сжимать содержимое для экономии места на диске”.

Рассмотренным способом можно создавать резервные копии файлов, содержащих документы, изображения, презентации и другие данные, созданные прикладными программами пользователя. Решение не подойдет в случае, когда необходимо создавать архивные копии исполняемых и системных файлов, позволяющие восстанавливать ОС в случае сбоя.

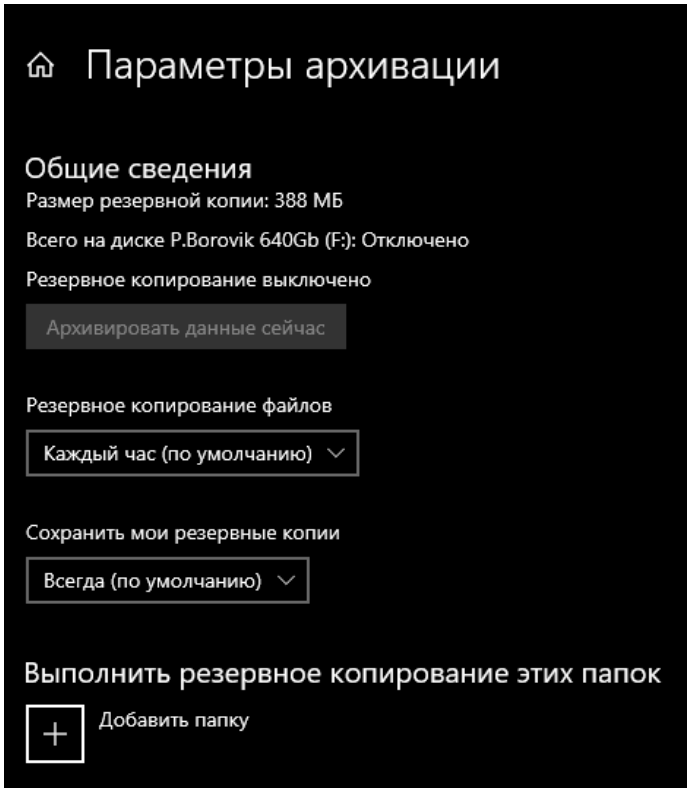


2.2. Резервное копирование файлов в Windows с помощью функции «Резервное копирование файлов”.

В Windows 10 есть функция «**Резервное копирование файлов**», которая автоматически выполняет резервное копирование файлов на выбранное устройство. Чтобы настроить ее, подключите к компьютеру внешнее запоминающее устройство. После подключения устройства, нажмите кнопку Пуск и выберите Параметры > Обновление и безопасность > Резервное копирование файлов. Затем нажмите на ссылку Другие параметры, после чего – периодичность копирования, срок копирования, а затем – Добавить папку (+) с файлами.

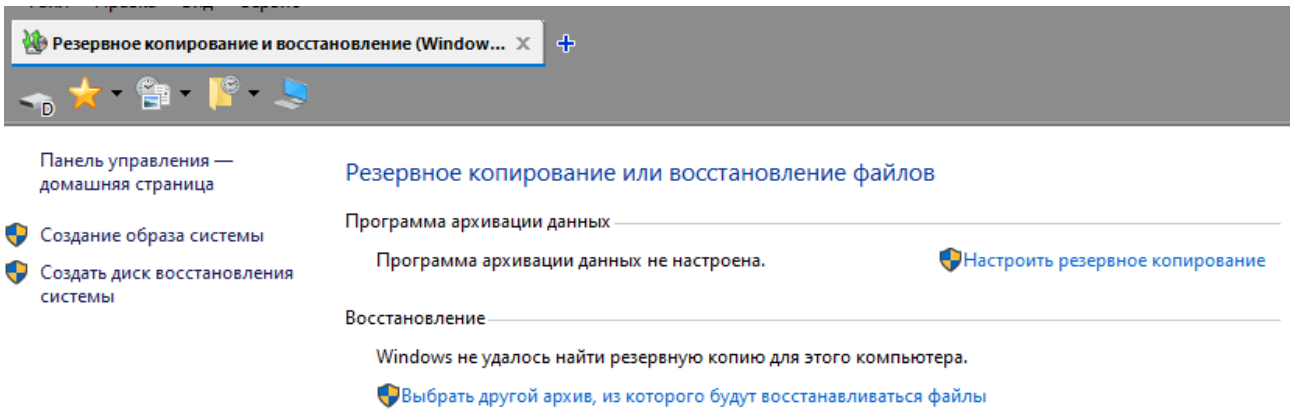
Для выбора внешнего запоминающего устройства следует нажать на ссылку «Просмотреть дополнительные параметры».

Для восстановления файлов следует использовать ссылку «Восстановить файлы из текущей резервной копии».



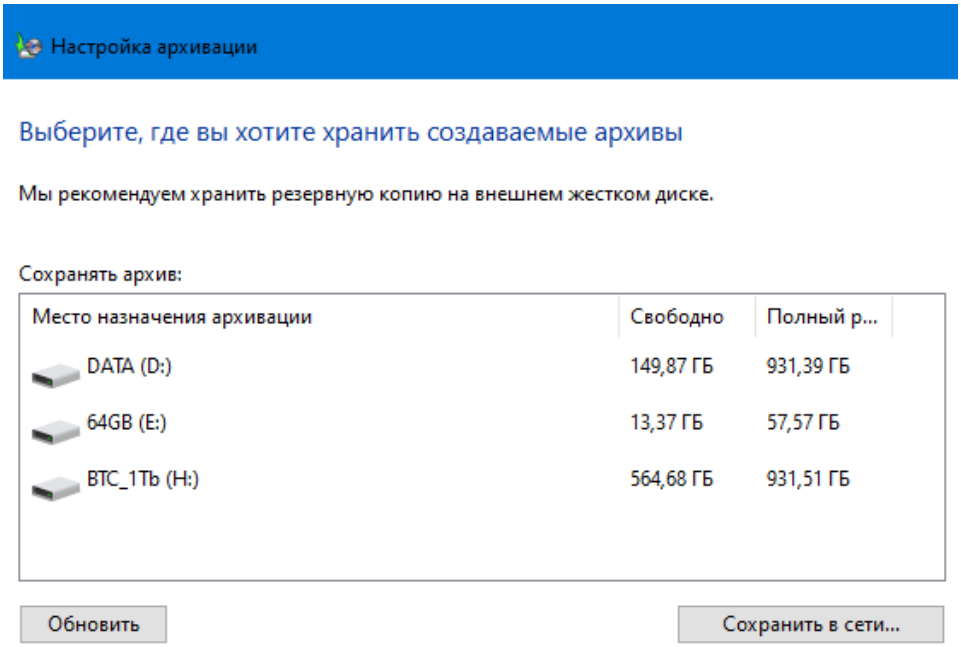
2.3. Резервное копирование файлов в Windows с помощью функции «Резервное копирование файлов”.

Этот инструмент можно найти на Панели управления в разделе «Резервное копирование или восстановление файлов».

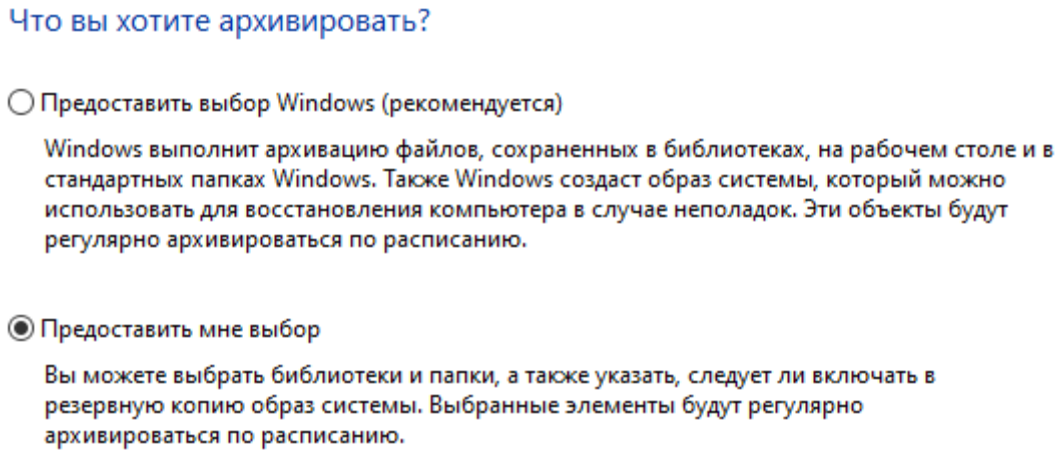


Для его настройки кликаем в окне «Резервное копирование или восстановление файлов» на ссылке «Настроить резервное копирование».

Для этого, Windows произведёт поиск подходящих устройств для сохранения резервной копии и предложит вам выбрать один из обнаруженных вариантов.

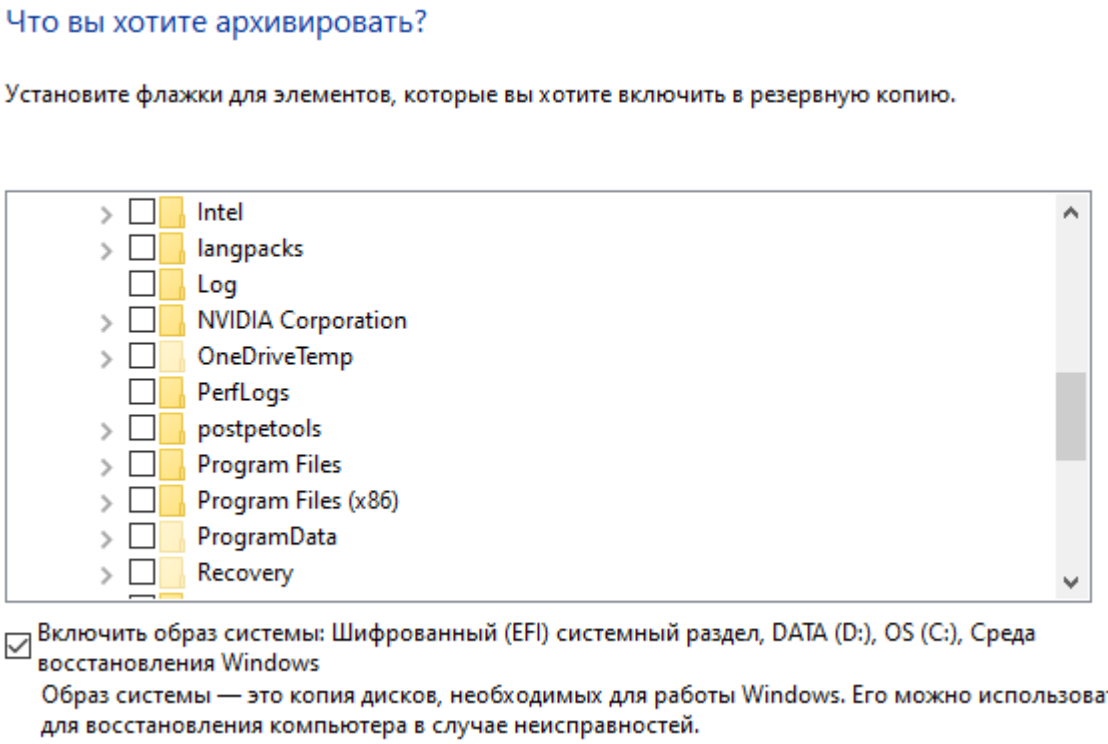


Выбрав необходимое устройство для сохранения резервной копии данных и нажав «Далее», вам будет предоставлено следующее меню, с помощью которого необходимо выбрать файлы или папки для резервирования.



Для более детального рассмотрения функции «Резервного копирования и восстановления» мы выберем второй вариант: «Предоставить мне выбор».

В случае выбора «Предоставить выбор Windows», Windows не сделает резервной копии папки Program Files, носителей, отформатированных в FAT, файлов которые находятся в «Корзине», а также временных файлов.



В предлагаемом далее окошке выбираем файлы и папки, которые необходимо включить в резервную копию. Это может быть, как «Библиотека пользователя» (папки «Документы», «Музыка», «Изображения» и т.д.) так и любой интересующий вас набор папок на локальном диске или весь диск целиком.

Если на компьютере создано несколько пользователей (в нашем случае на компьютере два пользователя: основной и «Тестовая»), то можно сделать бэкап данных всех пользователей, а не только того, под которым выполнен вход в систему.

Нажимаем на кнопку «Далее» и проверяем параметры архивации.

Обратите внимание: есть возможность изменить расписание выполнения архивации данных перейдя по ссылке «Изменить расписание».

Сохраняем Настройки расписания и нажимаем «Сохранить параметры и запустить архивацию», после чего наблюдаем за прогрессом создания нашей первой резервной копии данных.

Нажав «Показать подробные сведения» можно наблюдать процесс архивации данных более подробно.

После окончания процесса резервирования данных вы увидите два файла резервной копии и папку с образом системы.

Кликнув дважды на файле резервной копии данных можно восстановить данные или управлять местом на диске, которое занято резервной копией.

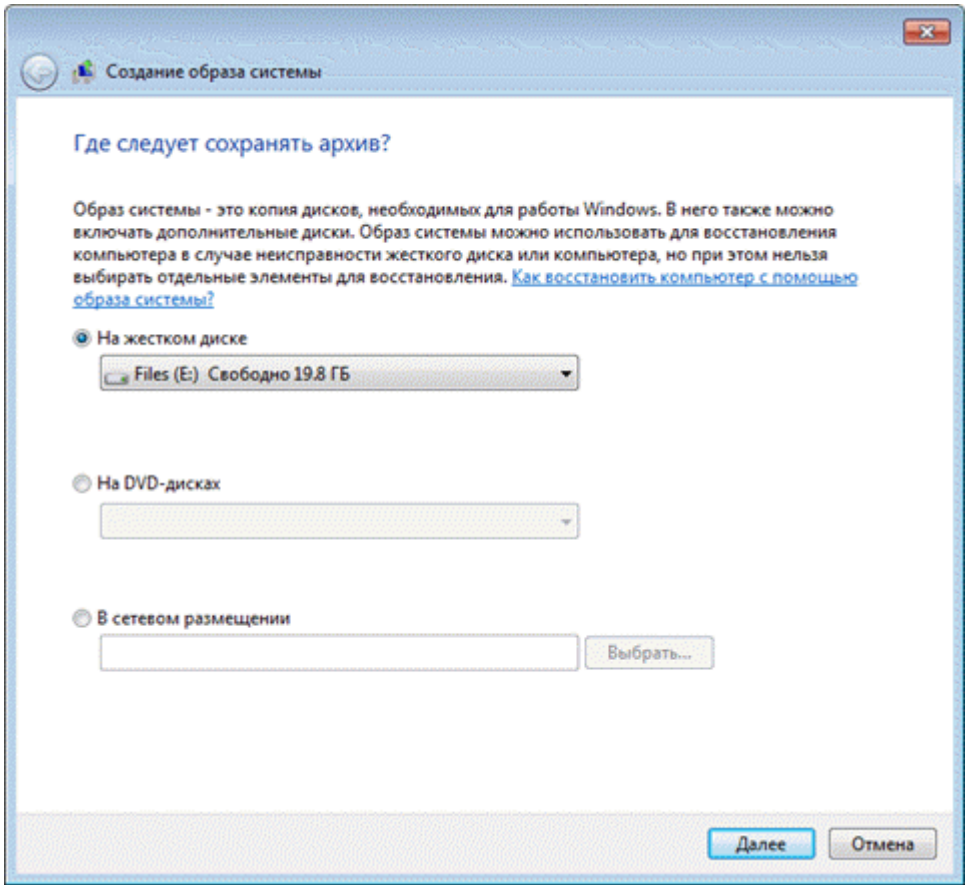
2.4. Создание образа системы

В отличие от файловых архивов, системный образ можно сохранить только на диске, отформатированном в файловую систему NTFS. Это

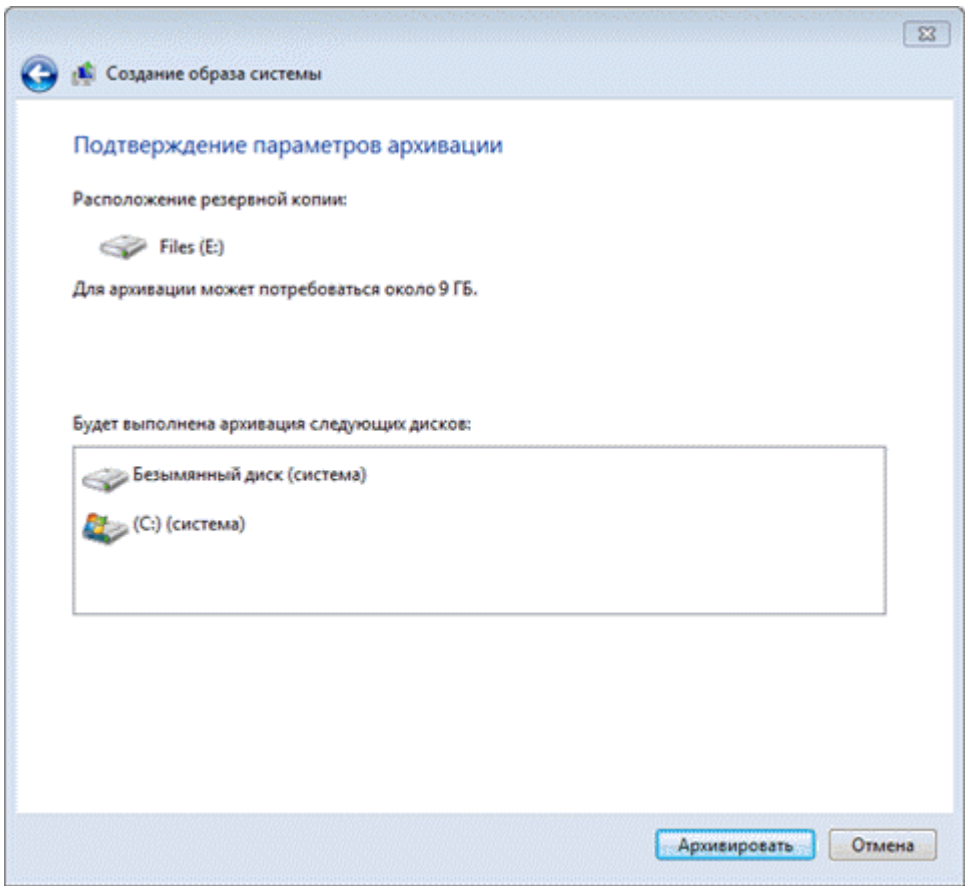
обусловлено тем, что образы представляют собой файлы в формате VHD, размер которых может превышать 4 Гб (предельный размер файла для FAT32).

Первый системный образ представляет собой полный снимок раздела, а последующие являются инкрементными, т. е. включают в себя лишь изменения по сравнению с предыдущим образом. Эта возможность, позволяющая сэкономить дисковое пространство, реализована с помощью теневых копий. Такой принцип создания образов применяется при их сохранении на внутренних, внешних и оптических дисках. Для внутренних и внешних дисков этот принцип действует до тех пор, пока на диске имеется достаточно места. Когда место заканчивается, создается полный образ, а все предыдущие удаляются. Что же касается сетевых дисков, то на них всегда создается полный образ, а старый образ при этом перезаписывается новым.

Рассмотрим создание первого образа. В левой панели элемента Архивация и восстановление нажмите ссылку Создание образа системы. Откроется окно с вариантами размещения образа.



На следующем шаге вы сможете выбрать разделы для архивации.



В образ автоматически включается служебный раздел со средой восстановления (Windows RE) и системный раздел. Исключить их из резервной копии нельзя. Если в системе имеются другие разделы, вы сможете выбрать их на этом шаге. Определившись с выбором разделов, нажмите кнопку **Архивировать**, чтобы начать процесс создания резервной копии.

Все следующие образы создаются точно так же. Они содержат только изменившиеся блоки. Для того чтобы снова создать полный образ системы, вам необходимо удалить существующие образы или перенести их на другой раздел. Вы также можете переместить их из корня диска во вложенные папки, однако примите к сведению, что в этом случае их не увидит программа.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 3.2»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

1. Создайте на диске D три пустых файла. Это могут быть документы Word, Excel, PowerPoint или другого формата. Создайте папку с именем «Важное» в папке «Документы» и сохраните эти файлы в папке «Важное».

1.1. Выполните резервное копирование папки «Важное» путем предварительного сжатия и последующего копирования в предварительно созданную папку Архив на диске D.

1.2. Выполните восстановление одного из файлов из полученного архива.

2. Выполните копирование данных файлов с помощью функции «Резервное копирование файлов» в папку Архив на диске D.

Настройте периодичность копирования (каждые 12 часов), срок копирования (1 год).

2.1. Выполните восстановление одного из файлов из полученного архива.

3. Выполните предыдущий пункт задания с помощью функции «Резервное копирование файлов” на Панели управления Windows.

Выполните сравнительный анализ указанного способа с предыдущим, самостоятельно сформулируйте выводы.

4. Создайте резервную копию системы. Настройте регулярное резервное копирование папки.

5. Продемонстрируйте результаты преподавателю.

6. Подготовьте ответы на контрольные вопросы (см. ниже).

Контрольные вопросы

1. Возможности архивации в Windows 10
2. Настройка параметров регулярного резервного копирования
3. Создание резервной копии файлов
4. Создание образа системы
5. Управление пространством
6. Расположение резервных копий
7. Содержимое файлового архива
8. Содержимое образа
9. Просмотр и удаление резервных копий
10. Образы системного раздела
11. Архивы пользовательских файлов