Тема: 3.4 Аппаратное и программное обеспечение защищенных компьютерных систем.

Учебные вопросы:
1. Антивирусное программное обеспечение.
2. Межсетевое экранирование.
3. Резервное копирование. Создание образа системы.

1. Антивирусное программное обеспечение. Онлайн-анализ подозрительных файлов и ссылок (URL) на предмет выявления вредоносного программного обеспечения (virustotal.com)

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).

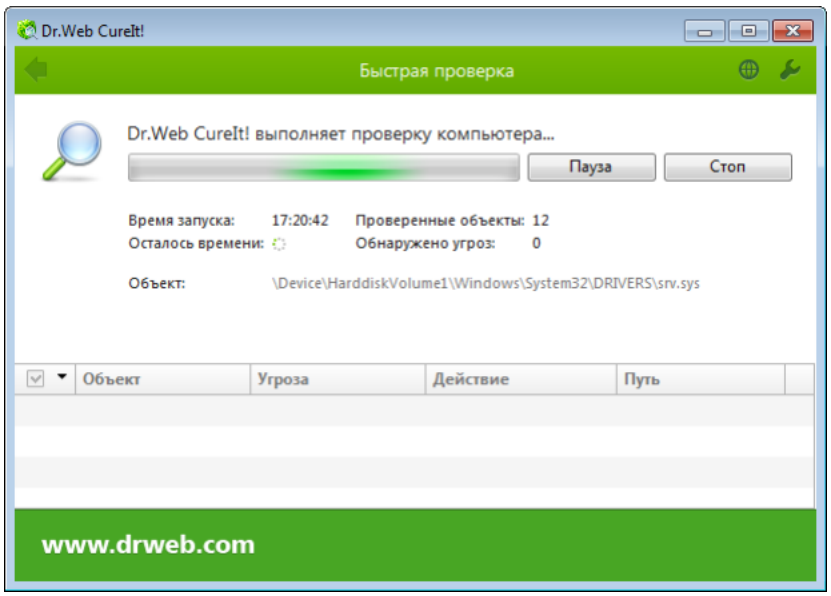

Рис. 2. Общая информация о ходе проверки, а также список обнаруженных угроз

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.

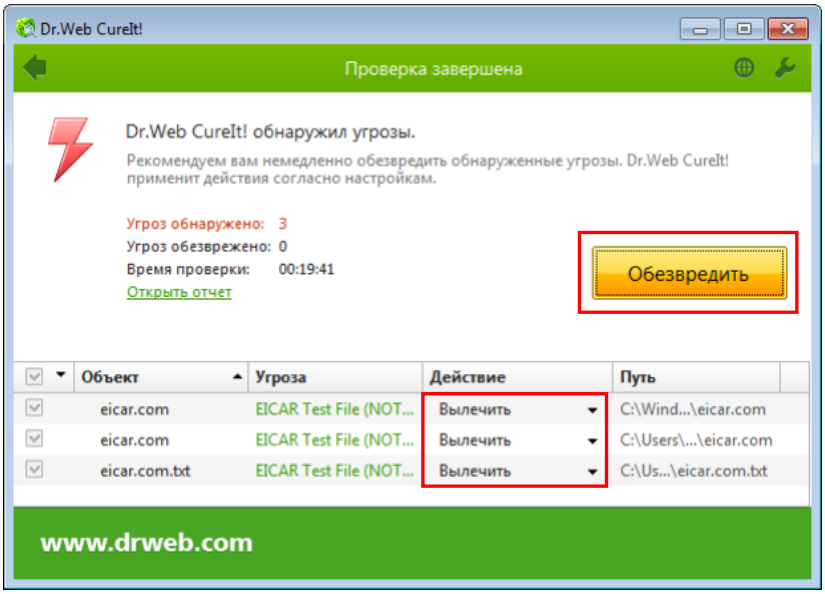

Рис. 3 Нейтрализация выявленных угроз утилитой Dr.Web CureIt

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.

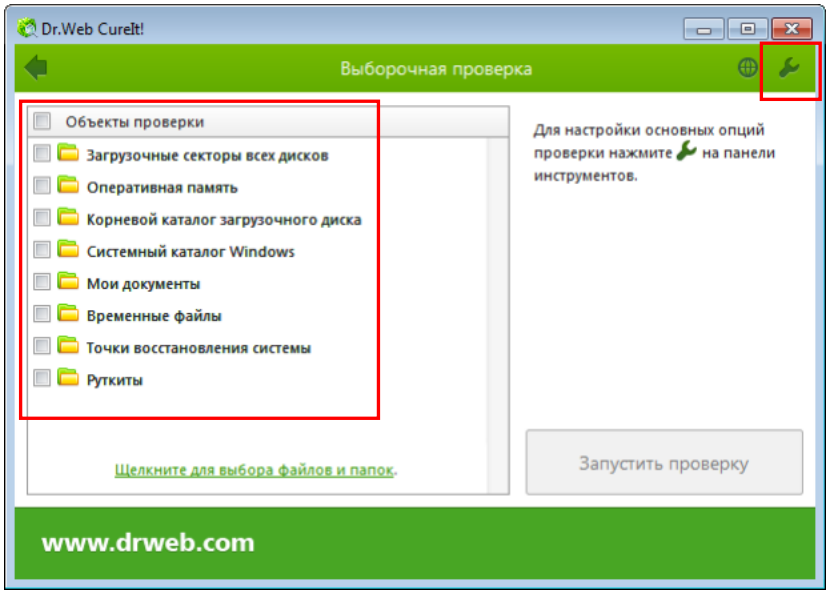

Рис. 5. Окно настройки выборочной антивирусной проверки с помощью утилиты Dr.Web CureIt

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 утиты;

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.

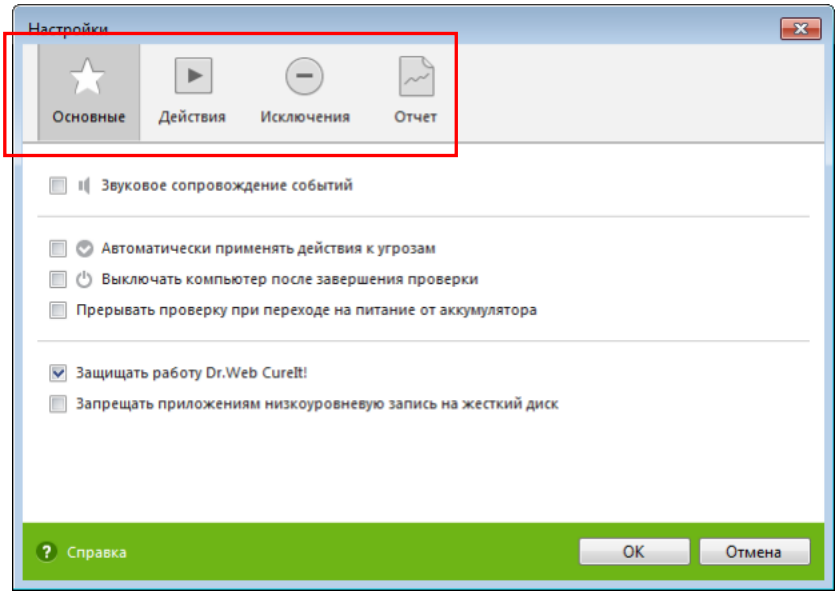

Рис. 6. Окно настройки параметров работы утилиты Dr.Web CureIt

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.

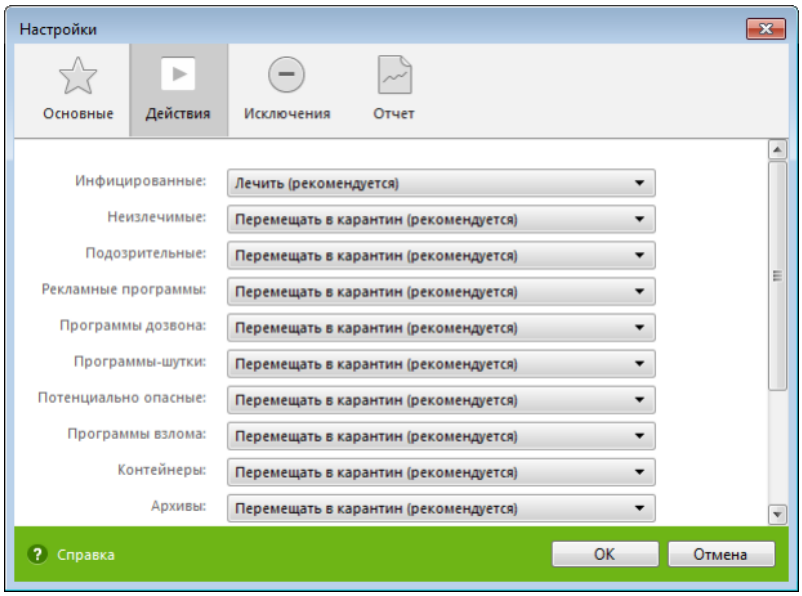

Рис. 7. Окно настройки параметров «Действия» утилиты Dr.Web CureIt

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

Действие	Описание
	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.

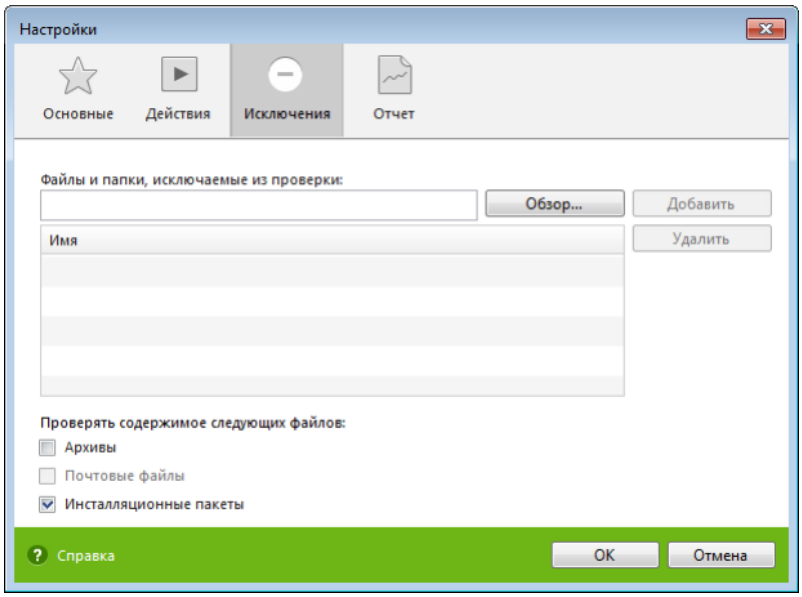

Рис. 8. Окно настройки параметров «Исключения» утилиты Dr.Web CureIt

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.

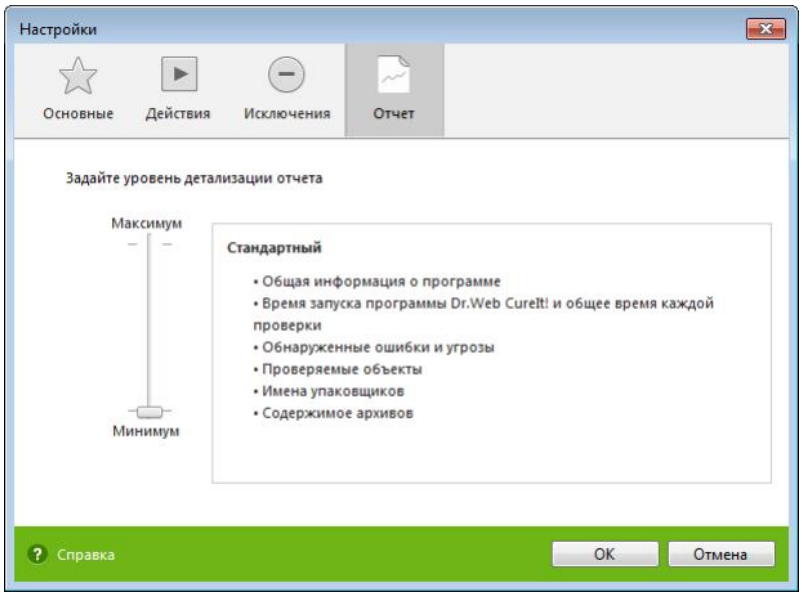

Рис. 9. Окно настройки параметров «Отчет» утилиты Dr.Web CureIt

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).

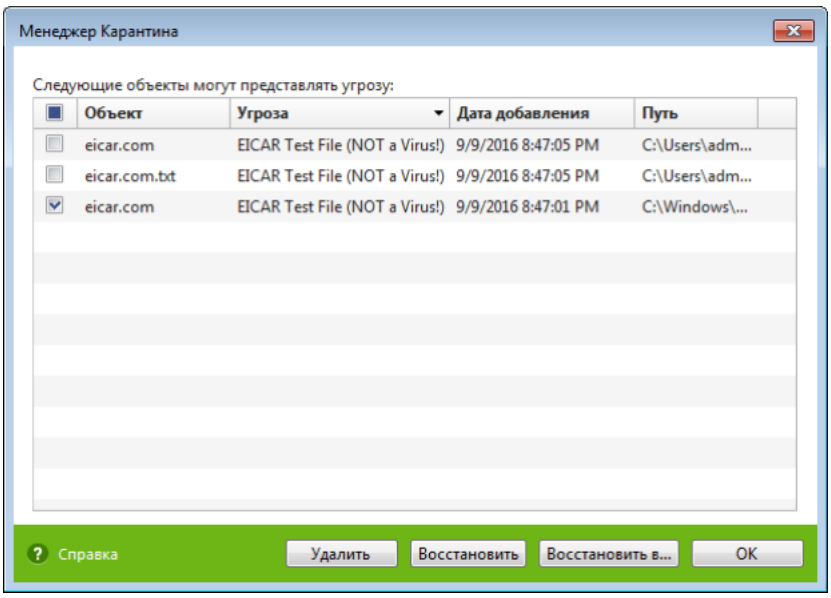

Рис. 10. Окно настройки параметров «Менеджер Карантина» утилиты Dr.Web CureIt

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».

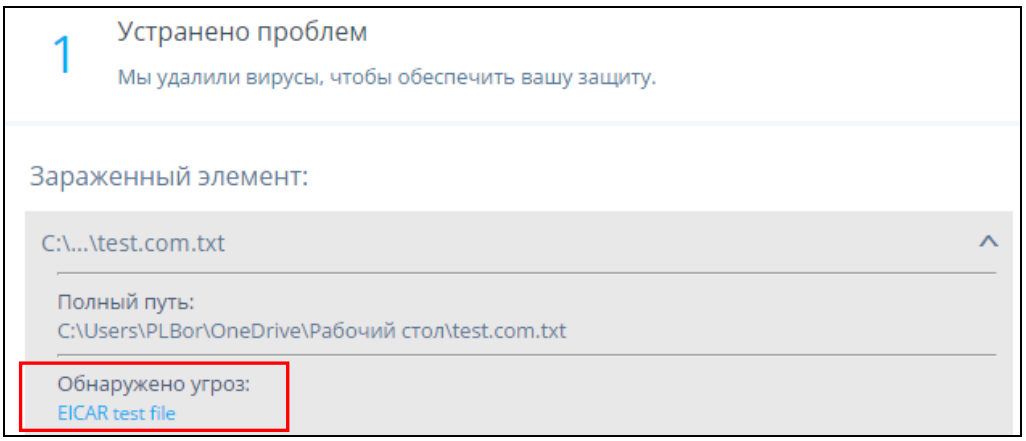

Рис. 11. Программа test.com обрабатывается большинством антивирусных программ как вирус

7) Запуск Dr.Web CureIt из командной строки

Иногда возникает ситуация, когда вредоносное программное обеспечение полностью блокирует запуск системы ПК (в том числе с любого съёмного носителя), при этом стандартные средства восстановления не работают по причине отсутствия образов (точек восстановления), а попытки обычной загрузки (запуска) Dr.Web CureIt или аналогов не представляются возможным.

В этом случае единственным вариантом решения данной проблемы может быть запуск Dr.Web CureIt в режиме командной строки.

Кроме того, запуск утилиты в режиме командной строки позволяет задать дополнительные настройки текущего сеанса сканирования (например, задать проверку инсталляционных пакетов; загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска; системных точек восстановления ОС; файлов, на которые ссылаются ярлыки и символьные ссылки; альтернативных потоков данных NTFS; поиск угроз в оперативной памяти, включая системную область ОС и др.), а также перечень проверяемых объектов в качестве параметров вызова.

Бывают также случаи, когда один файл заражен несколькими вирусами. В подобной ситуации файл будет оставаться зараженным даже после удаления одного из вирусов. Поддерживаемая утилитой Dr.Web CureIt и запускаемая только в режиме командной строки функция рекурсивного сканирования позволяет обеспечить полное излечение файлов. Вылечив файл, утилита продолжает его сканирование на наличие других вирусов.

Синтаксис команды запуска следующий:

[<путь_к_программе>][<имя_CureIt!-файла>] [<объекты>] [<ключи>]

Список объектов сканирования может быть пуст или содержать несколько элементов, разделенных пробелами. Если путь к объектам

сканирования не указан, поиск осуществляется в папке, где расположен файл Dr.Web CureIt.

Наиболее распространенные варианты указания объектов сканирования:

/LITE – произвести стартовую проверку системы, при которой проверяются оперативная память и загрузочные секторы всех дисков, а также провести проверку на наличие руткитов.

/FAST – произвести быструю проверку системы.

/FULL – произвести полную проверку всех жестких дисков и сменных носителей (включая загрузочные секторы).

Ключи – параметры командной строки, которые задают настройки программы. При их отсутствии сканирование выполняется с ранее сохраненными настройками (или настройками по умолчанию, если вы не меняли их). Ключи начинаются с символа косой черты / и, как и остальные параметры командной строки, разделяются пробелами.

Наиболее распространенные варианты указания объектов сканирования:

* – сканировать все жесткие диски;

C: – сканировать диск C;

D:\games – сканировать файлы в каталоге;

*C:\games** – сканировать все файлы и подкаталоги каталога C:\games.

Полный перечень основных ключей командной строки приведен в таблице 2.

Таблица 2

№ п/п	Ключ командной строки	Описание
1.	/AA	автоматически применять действия к обнаруженным угрозам
2.	/AR	проверять архивы. По умолчанию опция отключена
3.	/AC	проверять инсталляционные пакеты. По умолчанию опция отключена.
4.	/ARL:<число>	максимальный уровень вложенности проверяемого архива. По умолчанию – без ограничений.
5.	/ARS:<число>	максимальный размер проверяемого архива, в килобайтах. Если размер архива превышает максимальный, Dr.Web CureIt! не распакует и не проверит его. По умолчанию – без ограничений.
6.	/DR	рекурсивно сканировать директории (проверять поддиректории). По умолчанию опция включена.
7.	/FL:<имя_файла>	сканировать пути, указанные в файле.
8.	/FM:<маска>	сканировать файлы по маске. По умолчанию сканируются все файлы.
9.	/FR:<регулярное_выражение>	сканировать файлы по регулярному выражению. По умолчанию сканируются все файлы.
10.	/HA	производить эвристический анализ файлов и поиск в них неизвестных угроз. По умолчанию опция включена.
11.	/LN	сканировать файлы, на которые указывают ярлыки. По умолчанию опция отключена.
12.	/NOREBOOT	отменяет перезагрузку и выключение после сканирования

№ п/п	Ключ командной строки	Описание
13.	/NT	сканировать NTFS-потоки. По умолчанию опция включена
14.	/OK	выводить полный список сканируемых объектов, сопровождая незараженные пометкой OK. По умолчанию опция отключена.
15.	/PAL:<число>	уровень вложенности упаковщиков. По умолчанию – 1000.
16.	/RA:<имя_файла>	дописать отчет о работе программы в указанный файл. По умолчанию – отчет не создается.
17.	/RP:<имя_файла>	записать отчет о работе программы в указанный файл. По умолчанию – отчет не создается.
18.	/REP	сканировать по символьным ссылкам. По умолчанию опция отключена.
19.	/TB	выполнять проверку загрузочных секторов и главных загрузочных секторов (MBR) жесткого диска. По умолчанию опция отключена.
20.	/TM	выполнять поиск угроз в оперативной памяти (включая системную область Windows). По умолчанию опция отключена.
21.	/TR	сканировать системные точки восстановления. По умолчанию опция отключена.

При этом, параметры, включающие пробелы, необходимо заключать в кавычки. Например:

636frs47.exe /tm-

45hlke49.exe /tm- D:\test

10sfr56g.exe /OK- "D:\Program Files\"

Используя специальные модификаторы, можно также настроить подходящие действия для каждого типа угроз (C – *вылечить*, Q – *переместить в карантин*, D – *удалить*, I – *игнорировать*).

Перечень возможных настраиваемых действий для различных угроз приведен в таблице 3.

Таблица 3

№ п/п	Настраиваемый параметр действия для угрозы	Описание
1.	AAD:<действие>	действия для рекламных программ (возможные действия: DQI).
2.	/AAR:<действие>	действия с инфицированными архивами (возможные действия: DQI).
3.	/ACN:<действие>	действия с инфицированными инсталляционными пакетами (возможные действия: DQI).
4.	/AHT:<действие>	действия с программами взлома (возможные действия: DQI).
5.	/AIC:<действие>	действия с неизлечимыми файлами (возможные действия: DQ).
6.	/AIN:<действие>	действия с инфицированными файлами (возможные действия: CDQ).
7.	/ARW:<действие>	действия с потенциально опасными файлами (возможные

№ п/п	Настраиваемый параметр действия для угрозы	Описание
		действия: DQI).
8.	/ASU:<действие>	действия с подозрительными файлами (возможные действия: DQI).

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*;

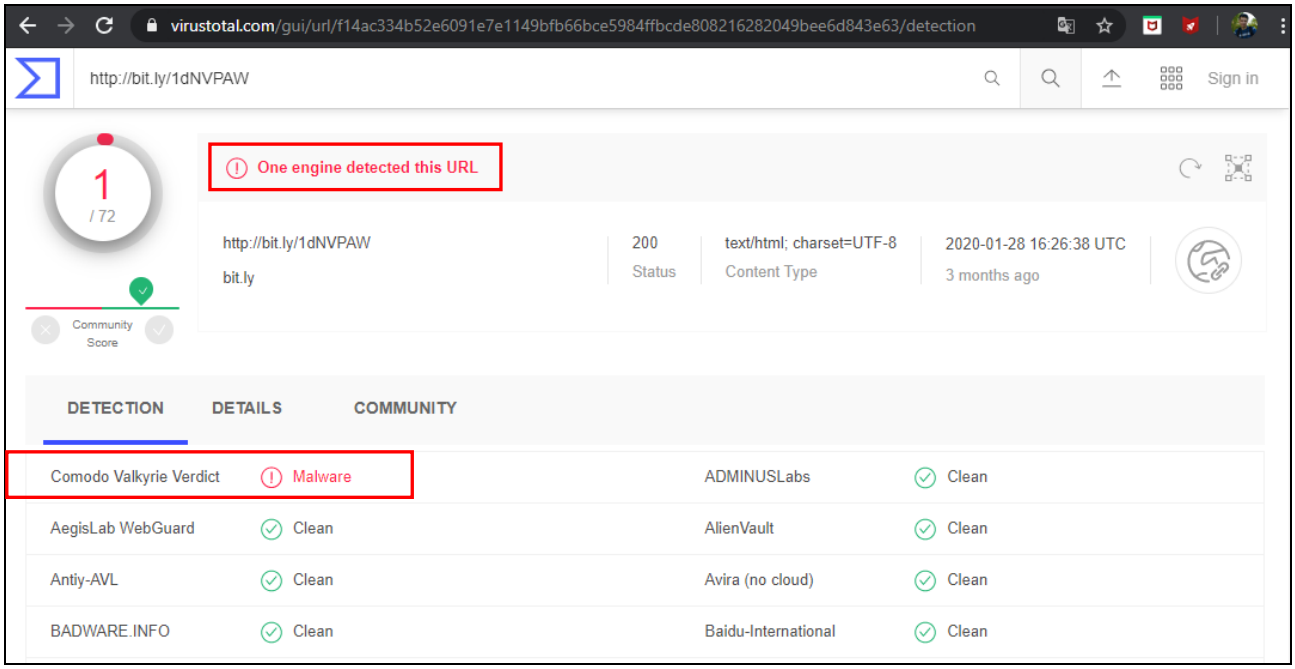

Рис. 13. Онлайн-сервис для анализа подозрительных файлов и ссылок (URL) на предмет выявления вредоносного программного обеспечения (virustotal.com)

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).

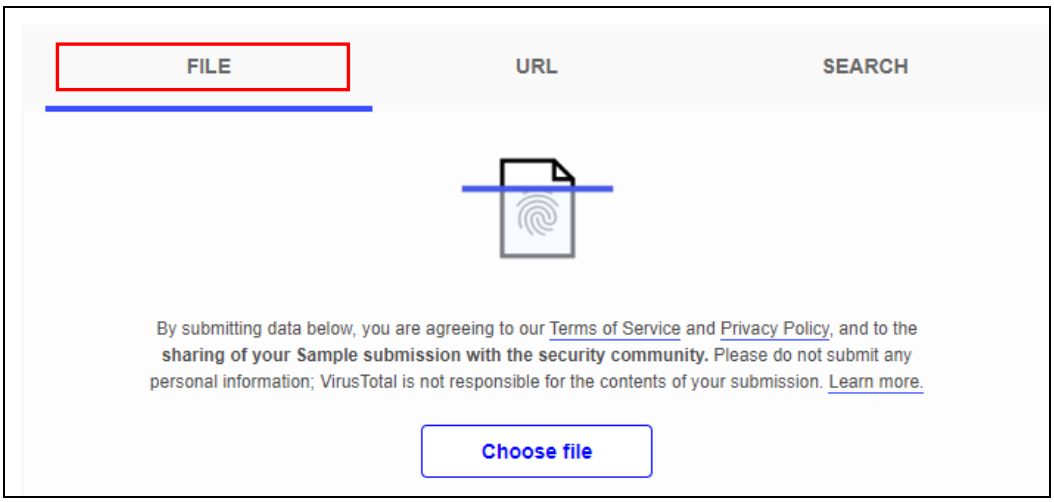

Рис. 14. Онлайн-сервис для анализа подозрительных файлов и ссылок (URL) на предмет выявления вредоносного программного обеспечения (virustotal.com)

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

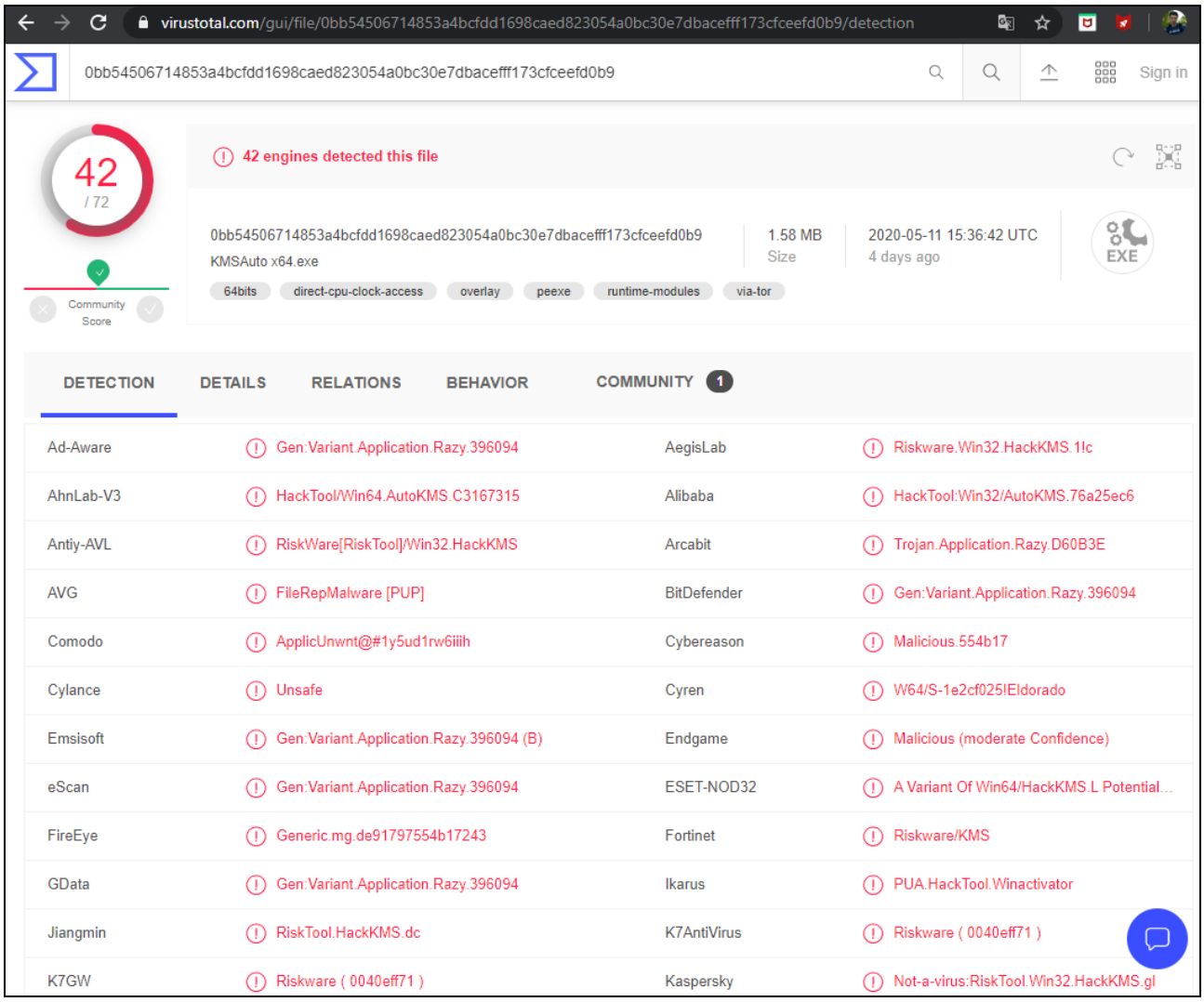

Рис. 15. Результаты проверки подозрительного файла с помощью онлайн-сервиса VirusTotal.

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.

Для проверки файлов можно также установить десктопное приложение VirusTotal Uploader (https://www.virustotal.com/static/bin/vtuploader2.2.exe) (рис. 16). С его помощью пользователь имеет возможность:

Upload Process Executable – выбрать подозрительный системный процесс и отправить его на проверку (данная возможность имеется только в приложении);

Select file(s) and upload – выбрать один или несколько файлов и отправить их на проверку (одновременно можно загрузить не более 5 файлов объемом до 20 Мб каждый);

Get and upload – загрузить файл и отправить его на проверку.

Дополнительно в настройках (*Options*) можно указать, как поступать с загружаемыми файлами – не хранить на диске (по умолчанию), помещать в папку *Temp* и удалять через некоторое время или хранить в отдельной папке.

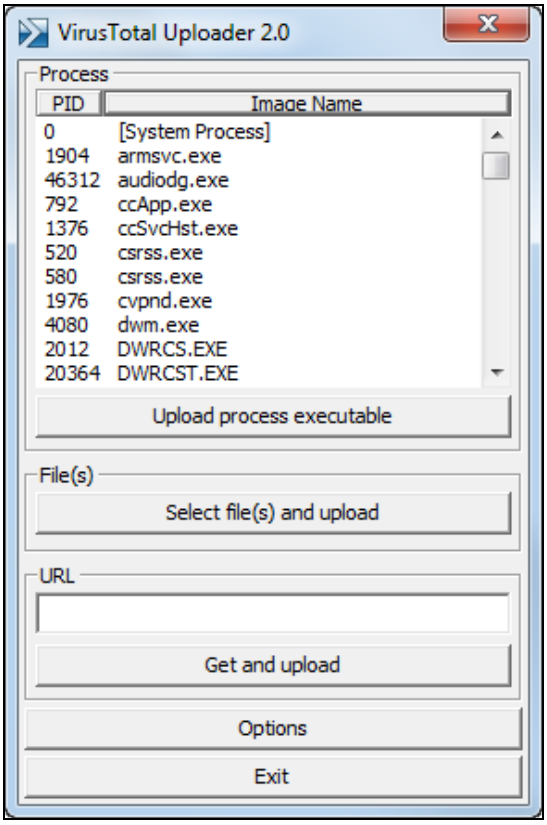

Рис. 16. Десктопное приложение VirusTotal Uploader для анализа подозрительных файлов и ссылок (URL)

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).

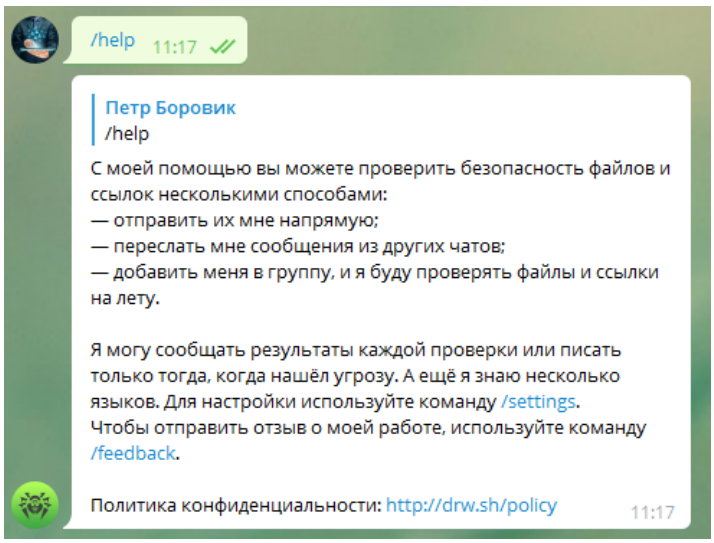

Рис. 19. Онлайн-сервис (бот) @drwebbot (https://telegram.me/drwebbot) для проверки ссылок URL на мобильном устройстве

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:

[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.

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;

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. Межсетевое экранирование. Изолированная среда исполнения с контролируемыми правами.

Краткие теоретические сведения:

1. Межсетевое экранирование в Windows 10: общие сведения

Одним из эффективных механизмом обеспечения информационной безопасности в распределенных вычислительных сетях является *межсетевое экранирование*, выполняющее функции разграничения информационных потоков на границе защищаемой сети. Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования

неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности.

Функции экранирования выполняет *межсетевой экран* (далее – МСЭ) или *брандмауэр* (firewall), под которым понимают программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Среди задач, которые решают МСЭ, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. МСЭ пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

За безопасность ОС Windows отвечает интегрированный МСЭ, функционирующий в двух основных режимах: *обычный* и *режим повышенной безопасности*.

В *обычном* режиме МСЭ в Windows автоматически настраивает правила и исключения, применяемые к исходящему и входящему трафику подключенной сети в зависимости от ее типа.

МСЭ Windows в *режиме повышенной безопасности* позволяет пользователю дополнительно создавать следующие правила:

отдельно настраивать правила как для входящего, так и для исходящего трафика;

создавать правила МСЭ на основе различных протоколов и портов;

настраивать правила обмена данными с сетью для служб (в обычном режиме МСЭ Windows позволяет настраивать правила только для приложений);

созданные правила могут относиться только к определенным IP-адресам в сети;

возможность пропуска только авторизованного трафика;

настраивать правила безопасности соединения.

По умолчанию МСЭ всегда запускается автоматически при старте системы, и пользователю не нужно предпринимать каких-либо действий. Но, в ряде случаев МСЭ может быть отключен. Для того, чтобы открыть и настроить его, наберите в поиске «Брандмауэр Защитника Windows» и выберите соответствие (рис. 20).

Появится окно программы, где вы увидите информацию о типе сети, к которой вы подключены: *частные*, *гостевые* или *общедоступные* (рис. 21).

Для включения (или отключения) МСЭ, вы должны сначала открыть его, затем в левом столбце нажать ссылку: «*Включение и отключение брандмауэра Защитника Windows*».

Откроется окно «*Настройка параметров для каждого типа сети*». Здесь вы можете указать, как включать или выключать брандмауэр Windows: для *частной сети*, для *общественной сети* или для обоих типов сетей (рис. 22).

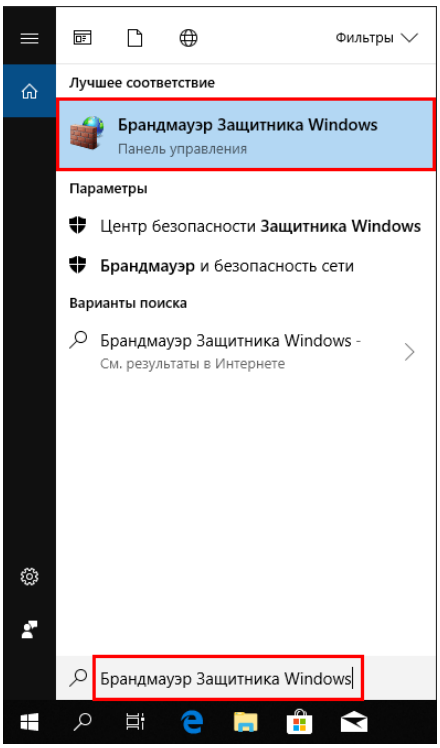

Рис. 20. Для того, чтобы открыть МСЭ в Windows 10, наберите в поиске «Брандмауэр Защитника Windows» и выберите лучшее соответствие

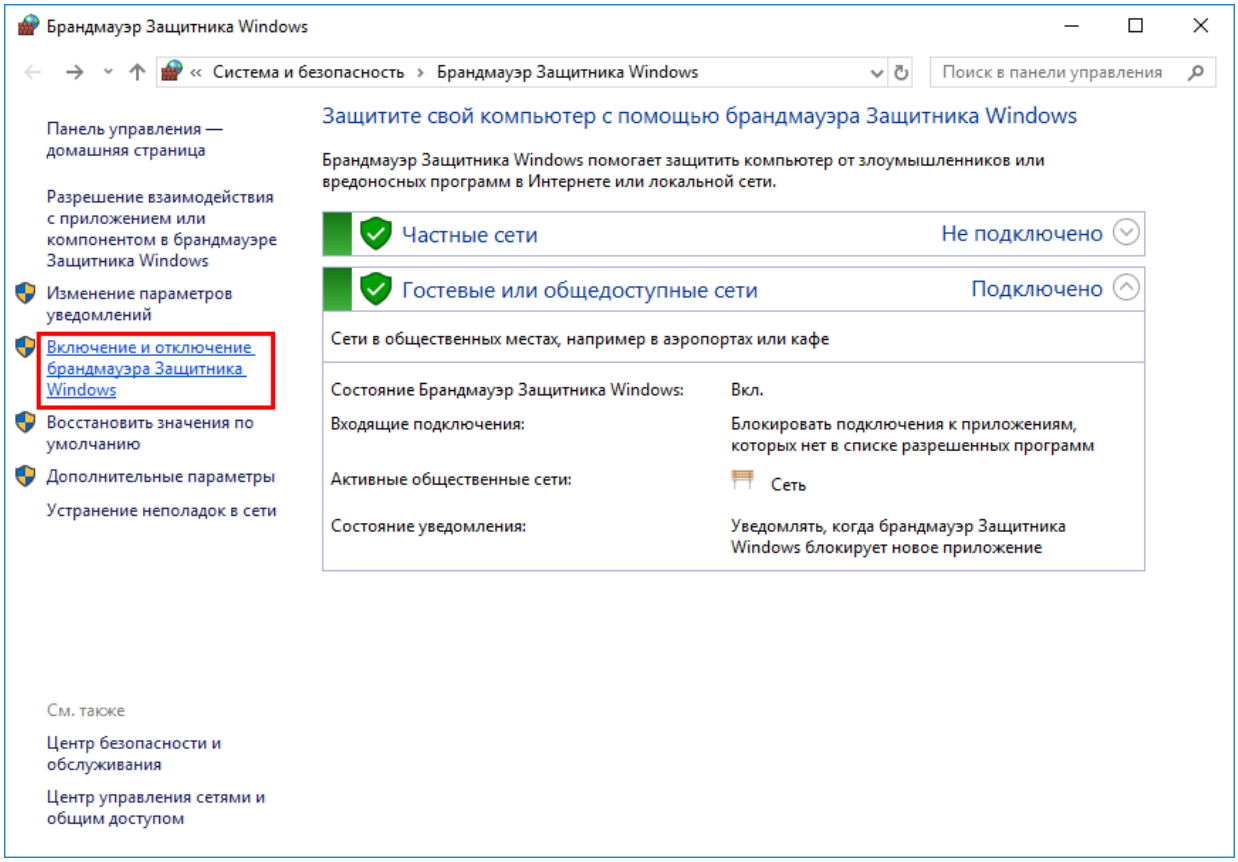

Рис. 21. Окно общих настроек МСЭ в Windows 10

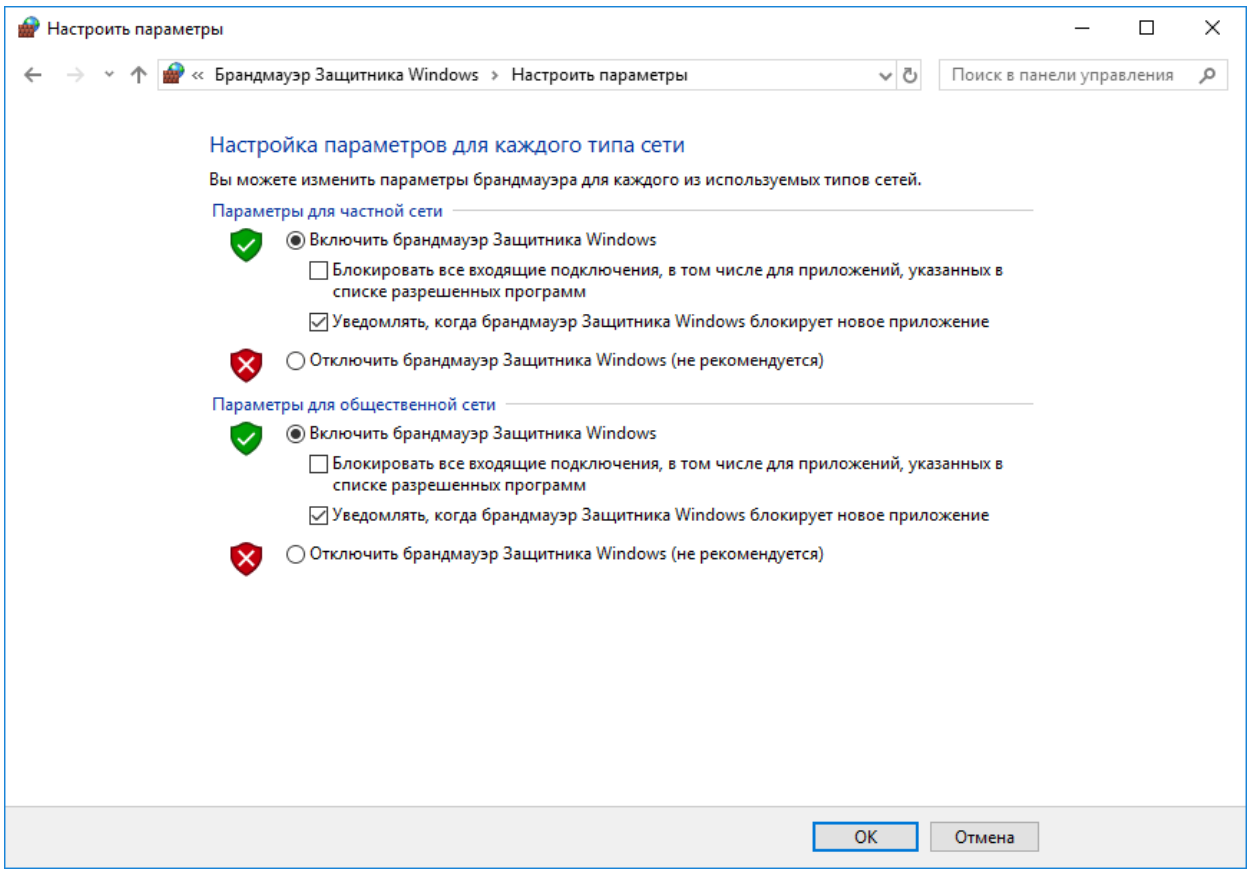

Рис. 22. Окно общих настроек МСЭ в Windows 10

Например, вы можете отключить МСЭ, когда подключены к доверенным частным сетям, таким которые находится в вашем служебном кабинете и включить, когда вы подключены к ненадежным общественным сетям (например, сети Интернет).

Если вы хотите включить его только для частных сетей, выберите «*Включить брандмауэр Защитника Windows*» в разделе «*Параметры для частной сети*».

Если вы хотите включить его только для общественных сетей, выберите «*Включить брандмауэр Защитника Windows*» в разделе «*Параметры для общественной сети*».

Если вы хотите включить его для всех типов сетей, выберите этот параметр в обоих разделах и нажмите «Ok».

Настройка правил и исключений в МСЭ

МСЭ позволяет пользователю с учетной записью администратора изменять список правил и исключений, применяемых для приложений и настольных программ.

Рассмотрим особенности настройки МСЭ на примере установления запрета конкретному приложению доступа в Интернет.

Откройте МСЭ, в столбце слева кликните по ссылке «*Разрешение взаимодействия с приложениями или компонентом в брандмауэре Защитника Windows*» (рис. 23).

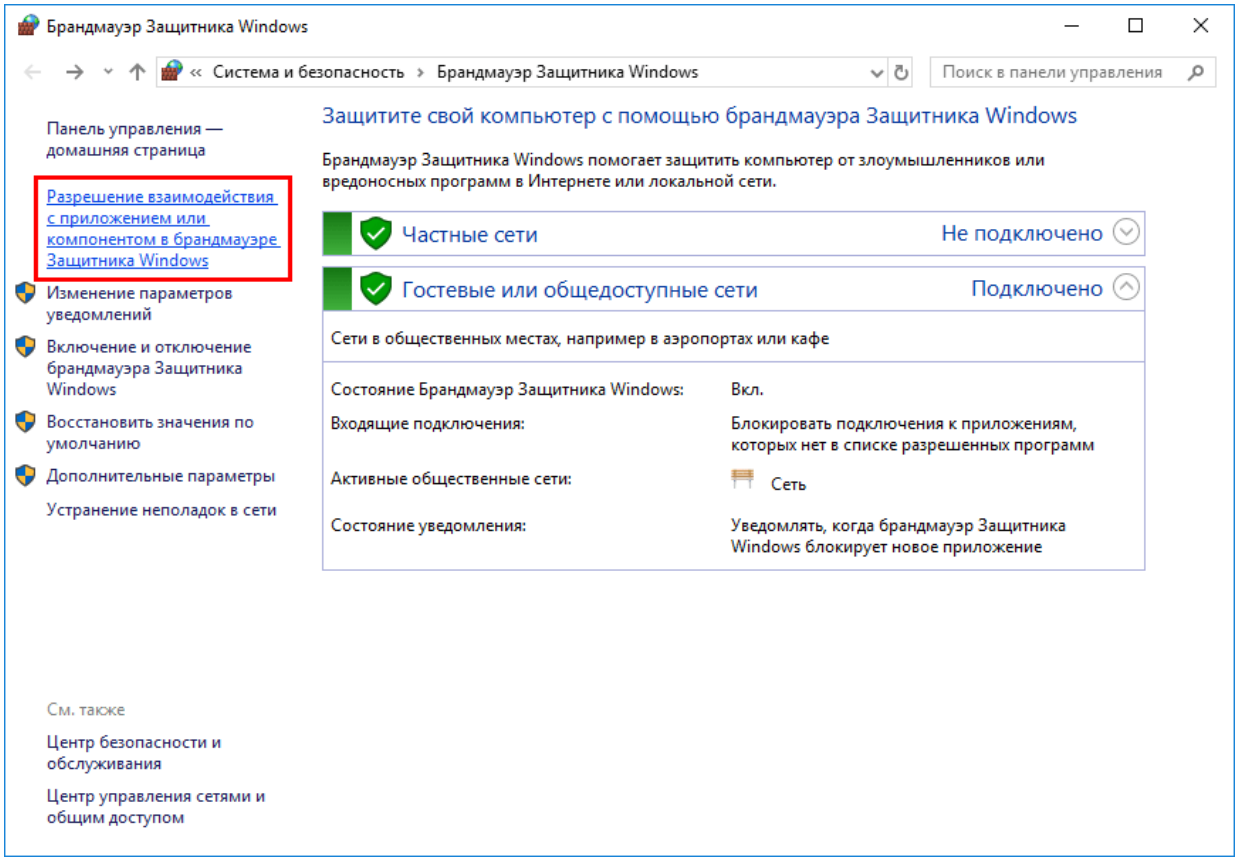

Рис. 23. Окно общих настроек МСЭ в Windows 10

Откроется окно со списком приложений, которым разрешен доступ в Интернет (рис. 24). На данный момент список неактивен, и вы можете только просматривать, какие приложения, функции и программы имеют правила.

Справа представлены два столбца: *Частная* и *Публичная* сеть. Если в столбце «*Частная*» имеется галочка, это означает, что доступ к сети предоставляется этому приложению, программе или функции, когда вы подключены к сети, которая установлена как частная. Если стоит галочка в столбце «*Публичная*», это значить, что доступ к сети предоставляется этому приложению, программе или функции, когда вы подключены к сети, которая установлена как публичная.

Для того, чтобы изменить этот список, нажмите на кнопку «*Изменить параметры*».

Теперь список больше не отображается серым цветом, и вам доступно редактирование любой из существующих записей (рис. 25).

Выберите нужный элемент, который вы хотите изменить (например, *bittorent*). Чтобы узнать больше об выбранном элементе, нажмите кнопку «*Сведения*».

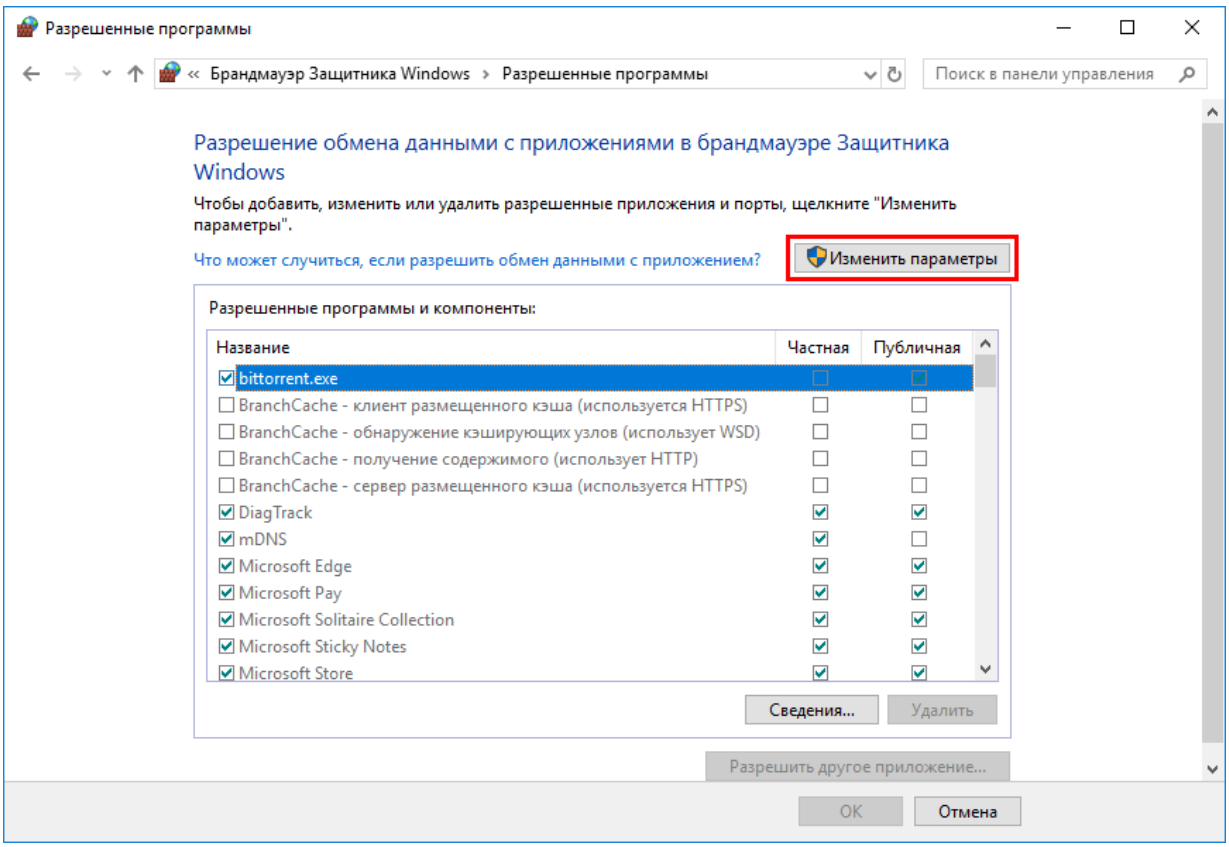

Рис. 24. Окно общих настроек МСЭ в Windows 10

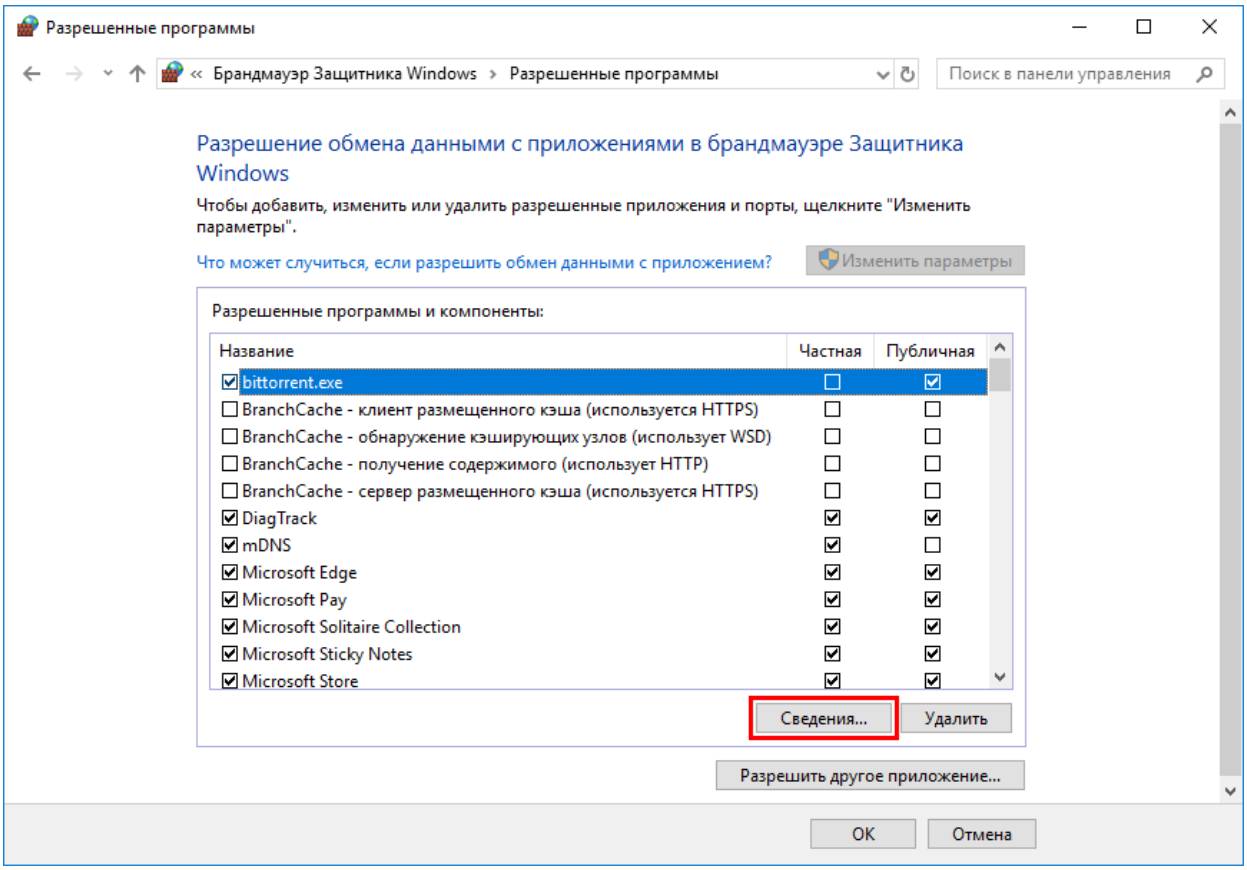

Рис. 25. Окно общих настроек МСЭ в Windows 10

Откроется информационное окно с описанием выбранного элемента или программы, ее название и путь расположения (рис. 26).

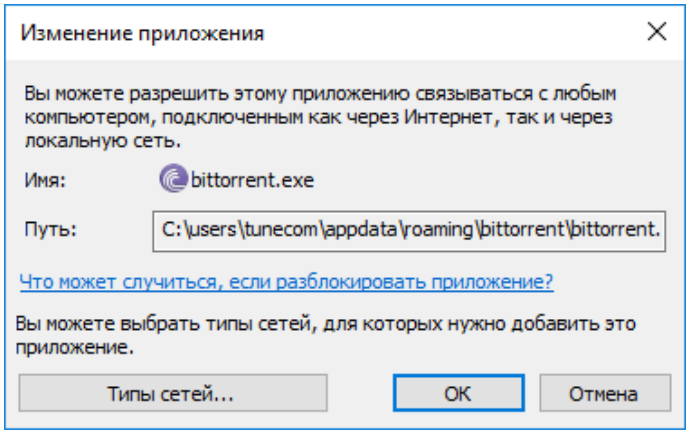

Рис. 26. Информационное окно с описанием выбранного элемента в МСЭ

Для того, чтобы заблокировать доступ к сети данному приложению, выберите, а затем снимите с него флажок (для блокировки доступа к любой сети) или один из флажков справа (частная или публичная), в зависимости от типа сети (рис. 27).

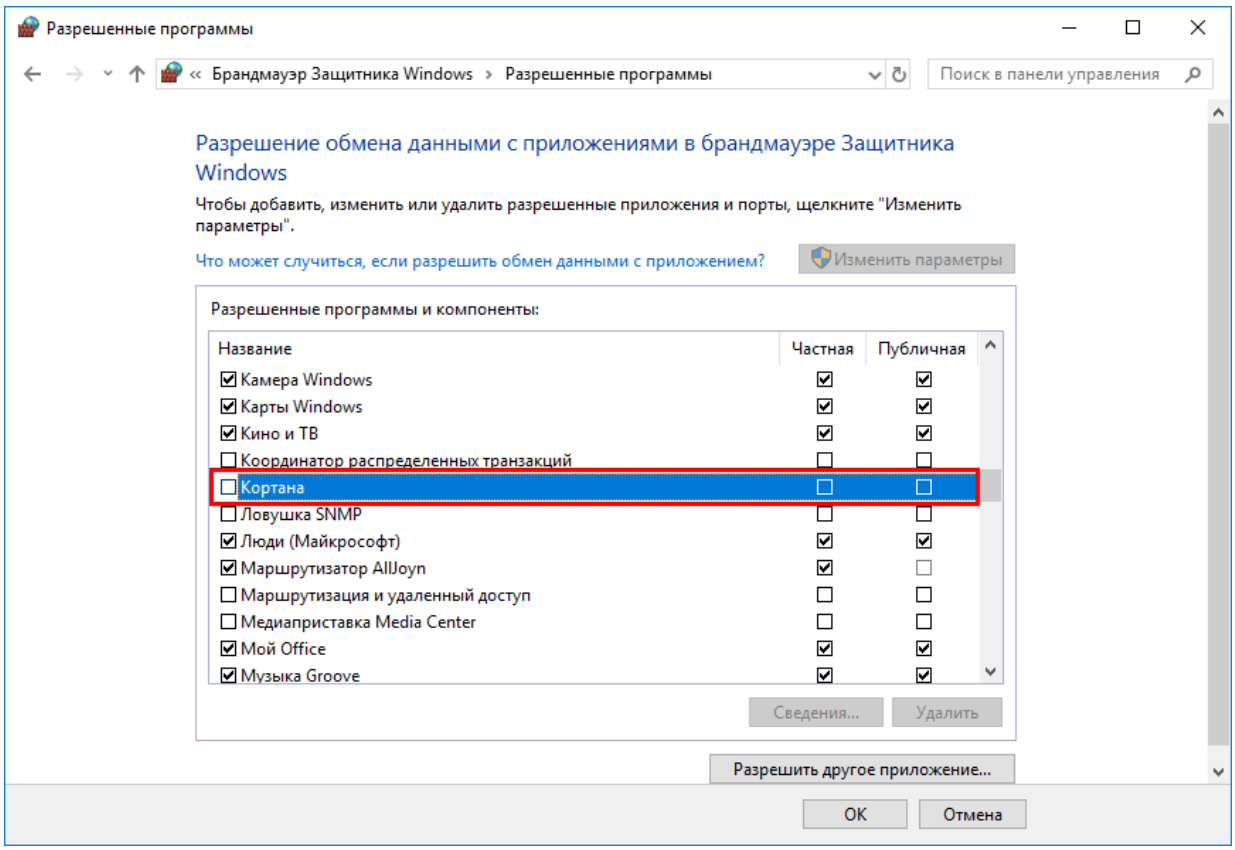

Рис. 27. Окно общих настроек МСЭ в Windows 10

Если нужно предоставить сетевой доступ приложению, программе или сервису, которые не имеют доступа в сеть, установите галочку рядом с ее именем и задайте тип сети.

По завершении настройки, для применения изменений нажмите кнопку «Ок».

Для того, чтобы предоставить доступ к сети приложению, которого нет в этом списке, нажмите на кнопку «*Разрешить другое приложение*».

В окне «*Добавление приложения*» нажмите кнопку «*Обзор*», перейдите в ее месторасположение и выберите исполняемый файл, затем нажмите кнопку «*Добавить*» (рис. 28).

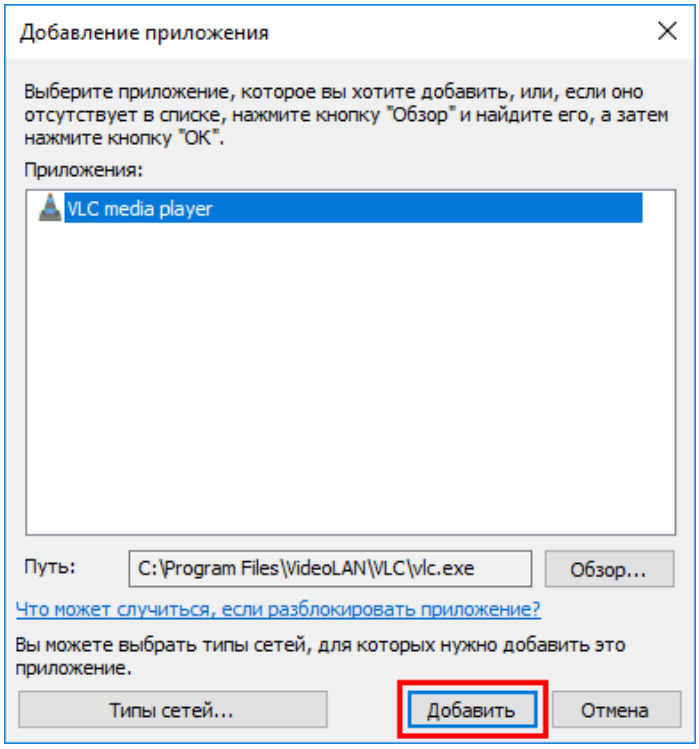

Рис. 28. Добавление приложения в список разрешенных программ для МСЭ

Вернитесь к списку разрешенных объектов и убедитесь, что программа, которую вы только что добавили теперь доступна (рис. 29).

Нажмите кнопку «Ок», чтобы применить свои настройки.

Внимание: при удалении программы из списка разрешенных элементов. она становится заблокированной по умолчанию, и при последующем ее использовании появится всплывающее уведомление от МСЭ, запрашивающее ваше одобрение для предоставления ему сетевого доступа.

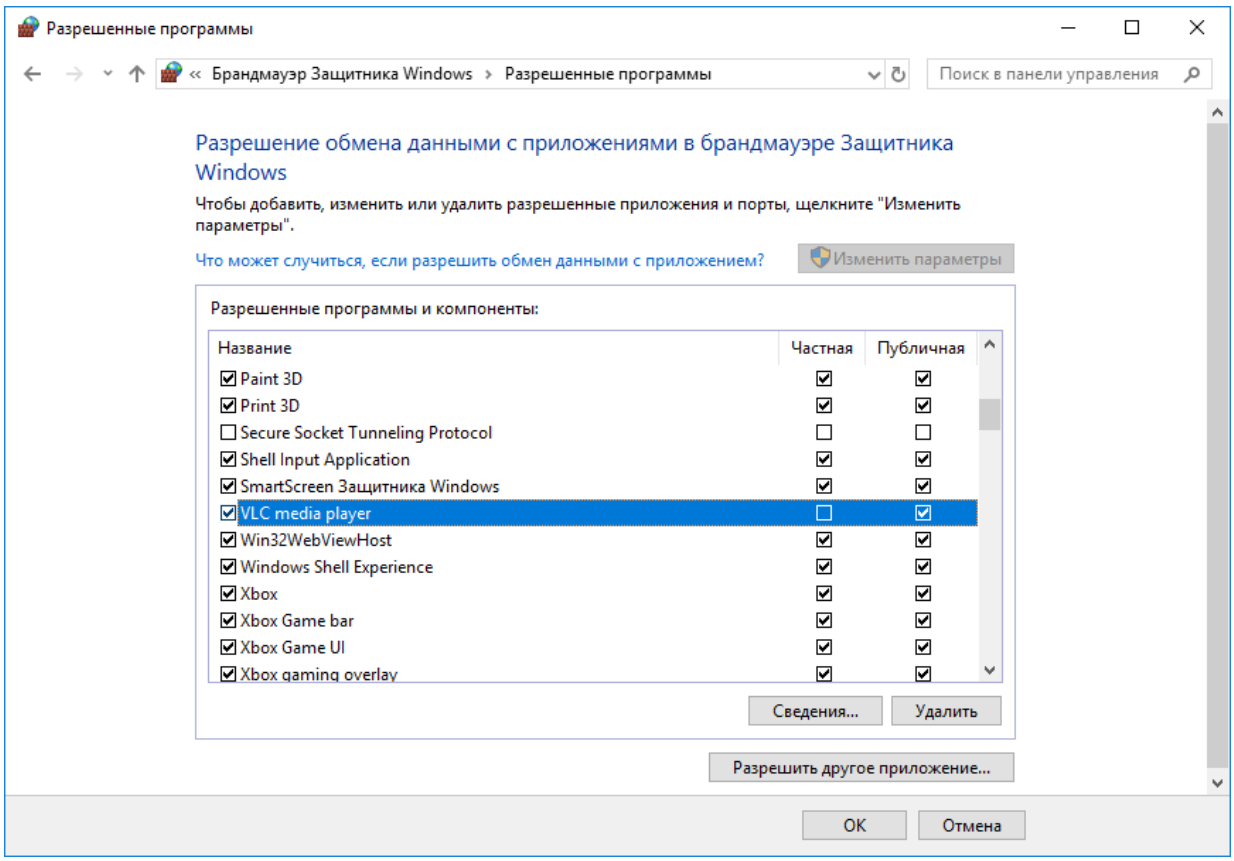

Рис. 29. Окно общих настроек МСЭ в Windows 10

Настройка параметров МСЭ в режиме повышенной безопасности

Режим повышенной безопасности МСЭ – это оснастка управления для брандмауэра, из которой вы можете управлять всеми его настройкам, правилами и исключениями.

Для получения доступа к расширенным настройкам откройте МСЭ, а затем нажмите на ссылку «*Дополнительные параметры*» в левом столбце экрана общих настроек (рис. 30).

МСЭ будет открыт в режиме повышенной безопасности (рис. 31). Рассмотрим особенности его настройки.

В средней части окна настроек (рис.31) МСЭ представлены параметры, характеризующие установки профилей (шаблонов настроек) и типов трафика.

Профиль домена: используются для компьютеров, подключенных к сети, содержащей доменные контроллеры, к которым принадлежат сетевые компьютеры. Когда компьютер успешно зарегистрирован в домене, он автоматически использует данный профиль.

Частный профиль: предназначен для служебных сетей, которые не подключены напрямую к Интернету, но находится за каким-то устройством безопасности, таким как маршрутизатор или другой аппаратный брандмауэр.

Общий профиль: обычно используется, когда компьютер подключен к публичной сети (Интернет или публичная точка доступа Wi-Fi). По умолчанию будут заблокированы все входящие подключения, которые не входят в список разрешенных.

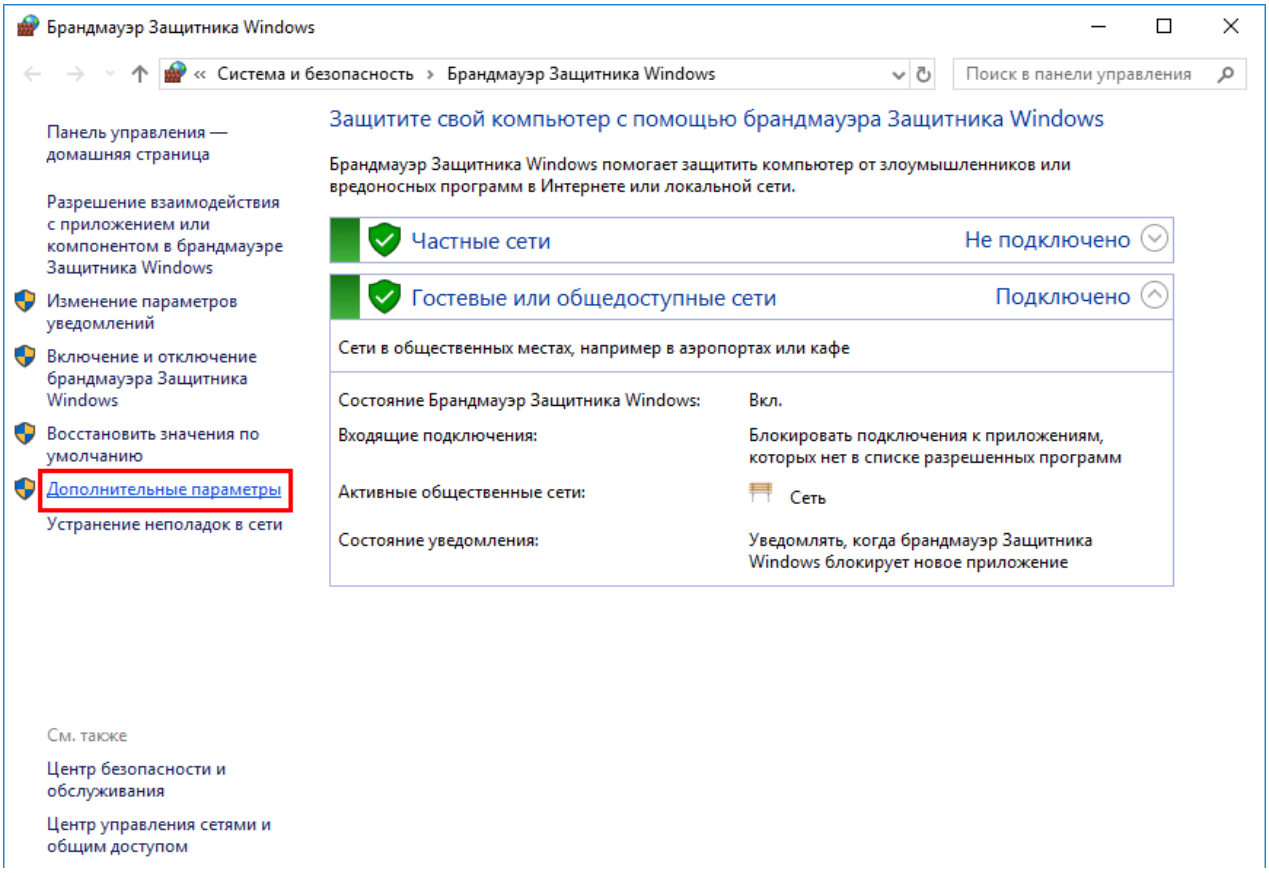

Рис. 30. Окно общих настроек МСЭ в Windows 10

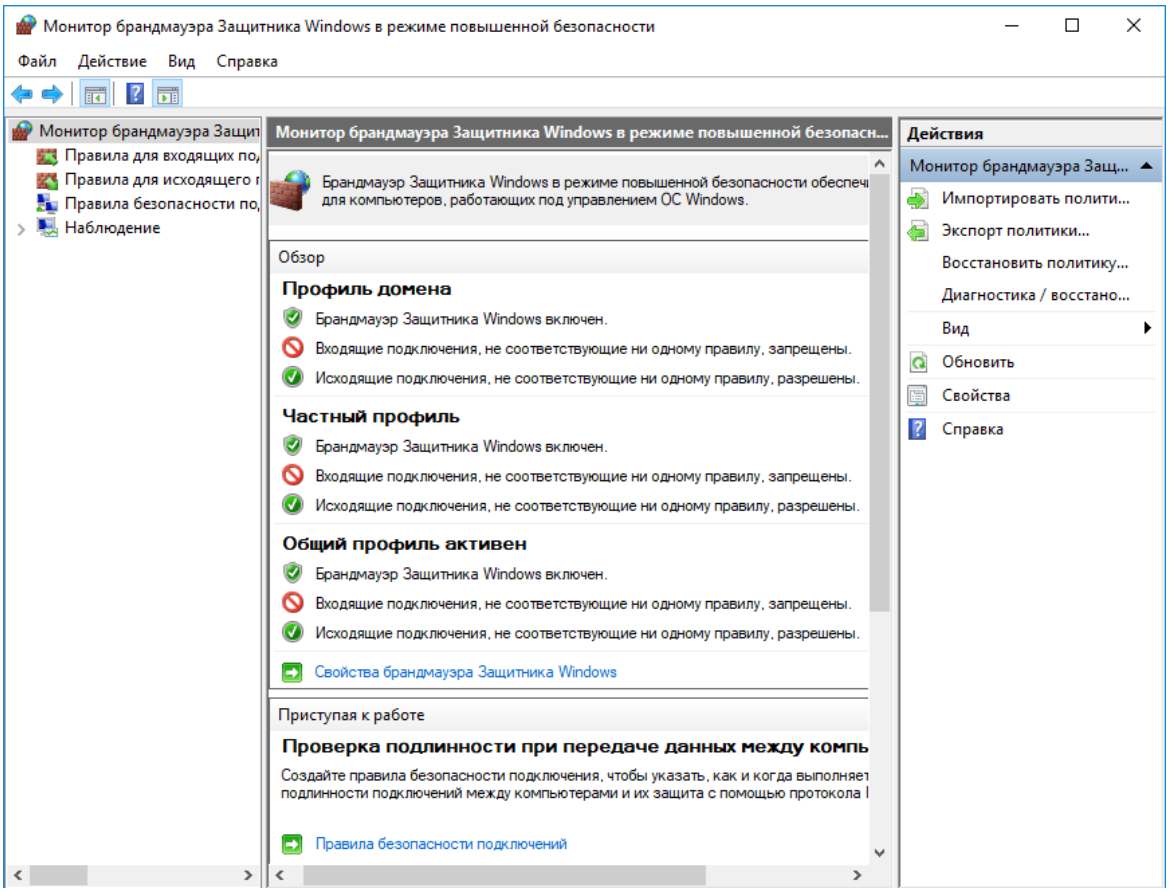

Рис. 31. Окно общих настроек МСЭ в Windows 10

Каждый профиль предполагает настройку определенных типов трафика.

Входящий – это трафик поступающий из сети или Интернета на компьютер или другое устройство. Например, если вы загружаете файл через uTorrent, скачивание этого файла фильтруется входящим правилом.

Исходящий – трафик, который исходит от вашего компьютера в сеть или Интернет. Например, запрос на загрузку веб-сайта в браузере – это исходящий трафик, и он фильтруется через исходящее правило.

Кроме того, режим повышенной безопасности МСЭ позволяет настраивать *правила безопасности подключений* – общие правила, которые используются для защиты трафика между двумя конкретными компьютерами и используется в очень контролируемых средах с особыми требованиями безопасности. В отличие от входящих и исходящих, применяющихся только к вашему компьютеру или устройству, правила безопасности подключения требуют, чтобы оба компьютера, участвующие в соединении и применяли одни и те же правила.

Для того, чтобы просмотреть правила определенного типа, выберите соответствующую категорию в столбце слева (рис. 32).

Правила МСЭ в режиме повышенной безопасности имеют следующие параметры, которые можно редактировать:

Имя – имя просматриваемого правила.

Группа – описывает приложение или функцию Windows, к которой принадлежит это правило. Например, правила, относящиеся к определенному приложению или программе, будут иметь имя приложения / программы в качестве группы. Правила, относящиеся к одной и той же сетевой функции, например «Общий доступ к файлам и принтерам», будут иметь название группы, к которой они относятся.

Профиль – сетевое местоположение / профиль, к которому применяется правило: домен частный или публичный (для сетей подразделения с сетевыми доменами).

Включено – сообщает вам, включено ли правило и применяется ли брандмауэром.

Действие – действие может «Разрешить» или «Блокировать» в зависимости от того, что должно делать правило.

Частота – указывает, переопределяет ли это правило существующее правило блока. По умолчанию все правила должны иметь значение «Нет» для этого параметра.

Программа – настольная программа, к которой применяется правило.

Локальный адрес – указывает, применяется ли правило только тогда, когда ваш компьютер имеет определенный IP-адрес или нет.

Удаленный адрес – указывает, применяется ли правило только при подключении устройств с определенными IP-адресами.

Протокол – разделяет сетевые протоколы, для которых применяется правило.

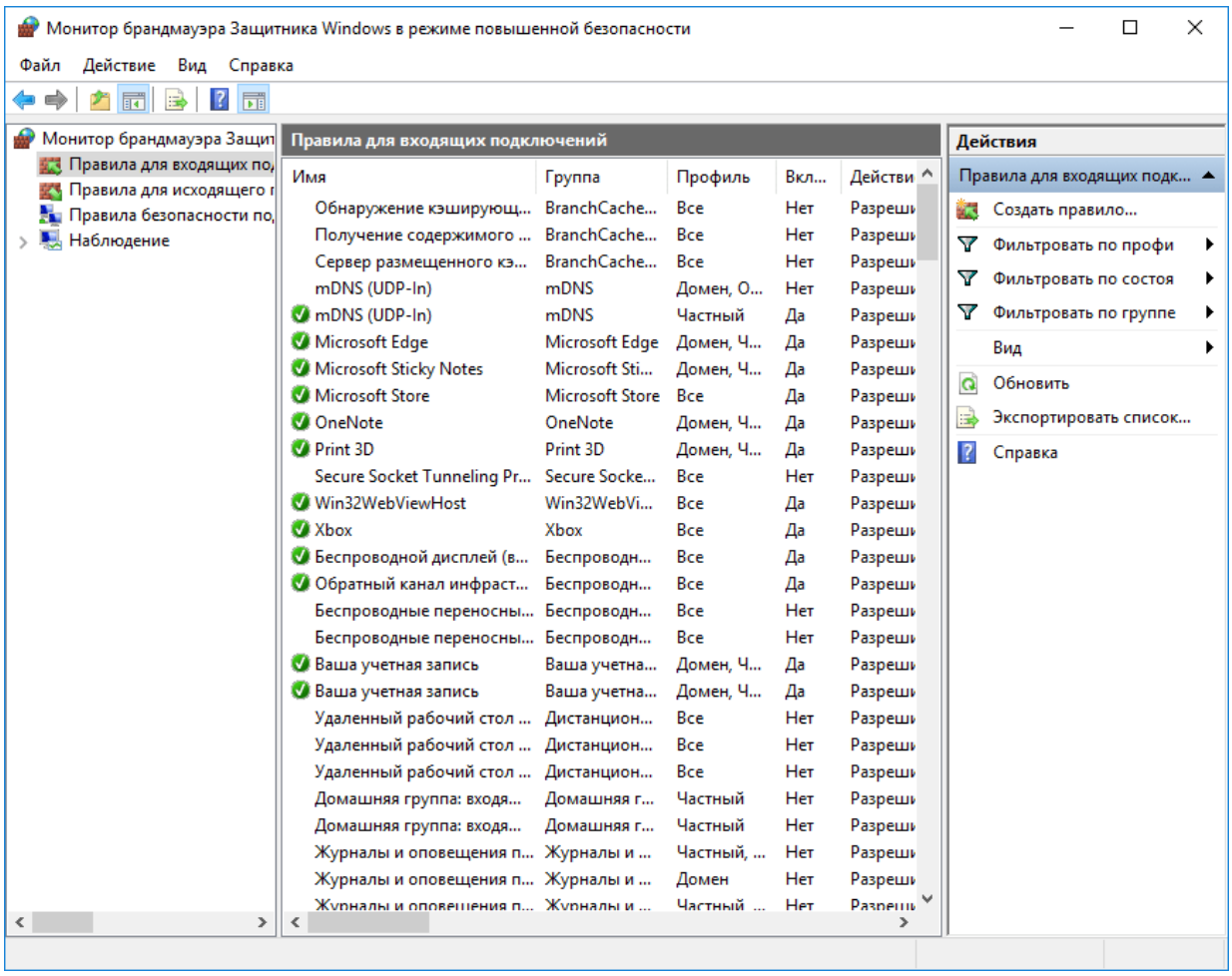

Рис. 32. Просмотр правил определенного типа в окне настроек МСЭ.

Локальный порт – указывает, применяется ли правило для соединений, сделанных на определенных локальных портах, или нет.

Удаленный порт – указывает, применяется ли правило для соединений, сделанных на определенных удаленных портах, или нет.

Авторизованные пользователи – учетные записи пользователей, для которых применяется правило (только для входящих правил).

Разрешенные компьютеры – компьютеры, для которых применяется правило.

Авторизованные локальные субъекты – учетные записи пользователей, для которых применяется правило (только для исходящих правил).

Локальный пользователь-владелец – учетная запись пользователя, установленная как владелец / создатель правила.

Пакет приложения – относится только к приложениям из Microsoft Store, и отображает имя пакета приложения, к которому применяется правило.

Для того, чтобы просмотреть активные правила брандмауэра и правила безопасности активных соединений, нажмите на ссылку «Наблюдение». Откроется окно с соответствующей информацией о состоянии МСЭ (рис. 33). Здесь вы можете посмотреть, какие одноранговые узлы подключены к вашему

ПК и какой пакет защиты использовался ОС для формирования политики безопасности.

Создадим *исходящее правило* на примере блокировки доступа к сети и Интернет для приложения Skype в случае подключения к ненадежным общедоступным сетям.

Для этого перейдите в «*Правила для исходящего подключения*» и нажмите «*Создать правило*» в столбце справа (рис. 34).

Откроется диалоговое окно «*Мастер создания правила для нового исходящего подключения*» (рис. 35)

На первом шаге мастера («Тип правила») предоставляется возможность осуществить следующий выбор:

Для программы – правило управляющее конкретной программой

Для порта – правило управляющее подключениями для порта TCP или UDP.

Предопределенные – правило, контролирующее подключения, выполняемые определенной службой или функцией Windows.

Настраиваемые – настраиваемое правило, которое может блокировать все программы и порты или определенную комбинацию.

В нашем случае выбираем «*Для программ*» и нажимаем «*Далее*».

На втором шаге мастера предлагается выбрать *все программы* или определенную программу, указав ее месторасположение.

Выбираем исполняемый файл программы, которую хотим заблокировать (Skype.exe) и переходим «*Далее*» (рис. 36).

На третьем шаге указываем действие, которое необходимо предпринять:

Разрешить подключение – включает как защищенные IPSec, так и соединения без защиты.

Разрешить безопасное подключение – включает только подключения с проверкой подлинности с помощью IPSec. Вы можете указать тип аутентификации и шифрования, которые вы хотите применить, нажав «*Настроить*».

Блокировать подключение – блокирует соединение, независимо от того, является ли оно безопасным или нет.

Выбираем «*Блокировать подключение*» и нажимаем «*Далее*» (рис. 37).

На шаге «*Действие*» следует выбрать, для каких профилей применяется правило:

Доменный – применяется при подключении компьютера к домену своей организации.

Частный – применяется, когда компьютер подключен к частной сети, например домашней или рабочей.

Публичный – применяется если компьютер подключен к ненадежной общественной сети.

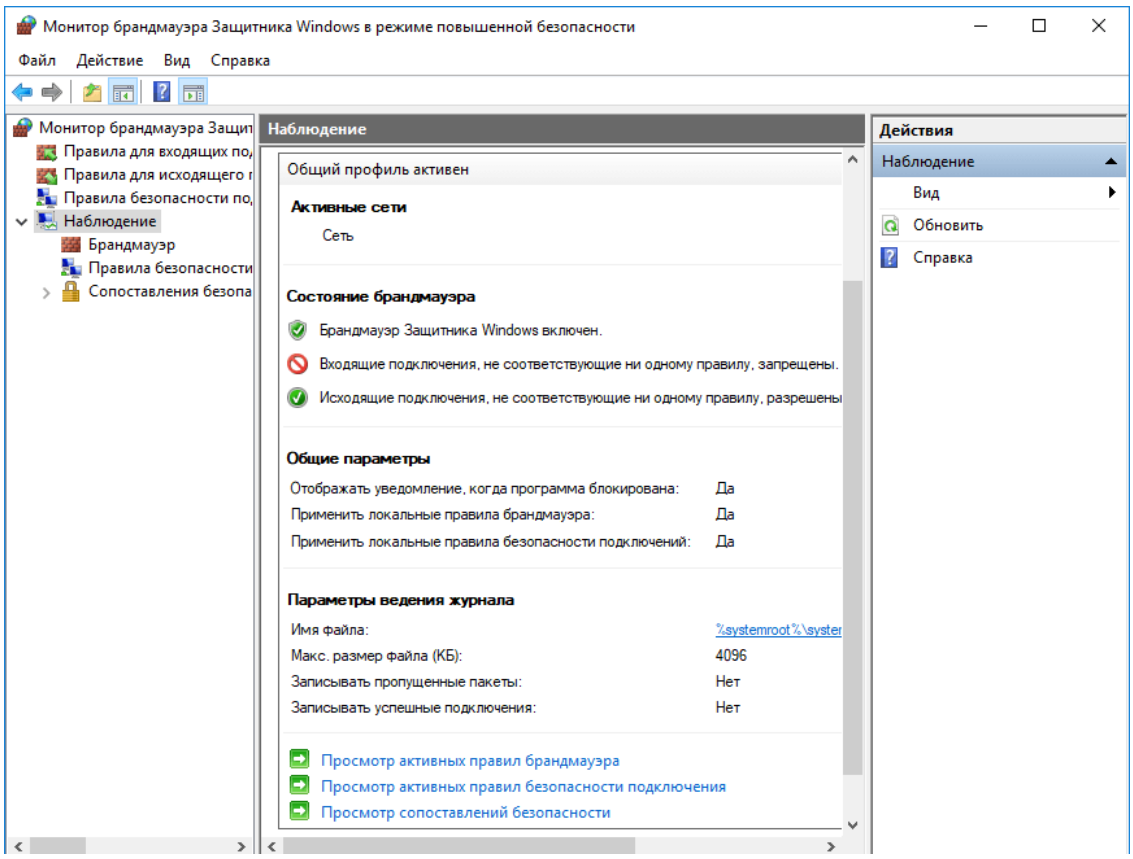

Рис. 33. Просмотр активных правил МСЭ и правил безопасности активных соединений

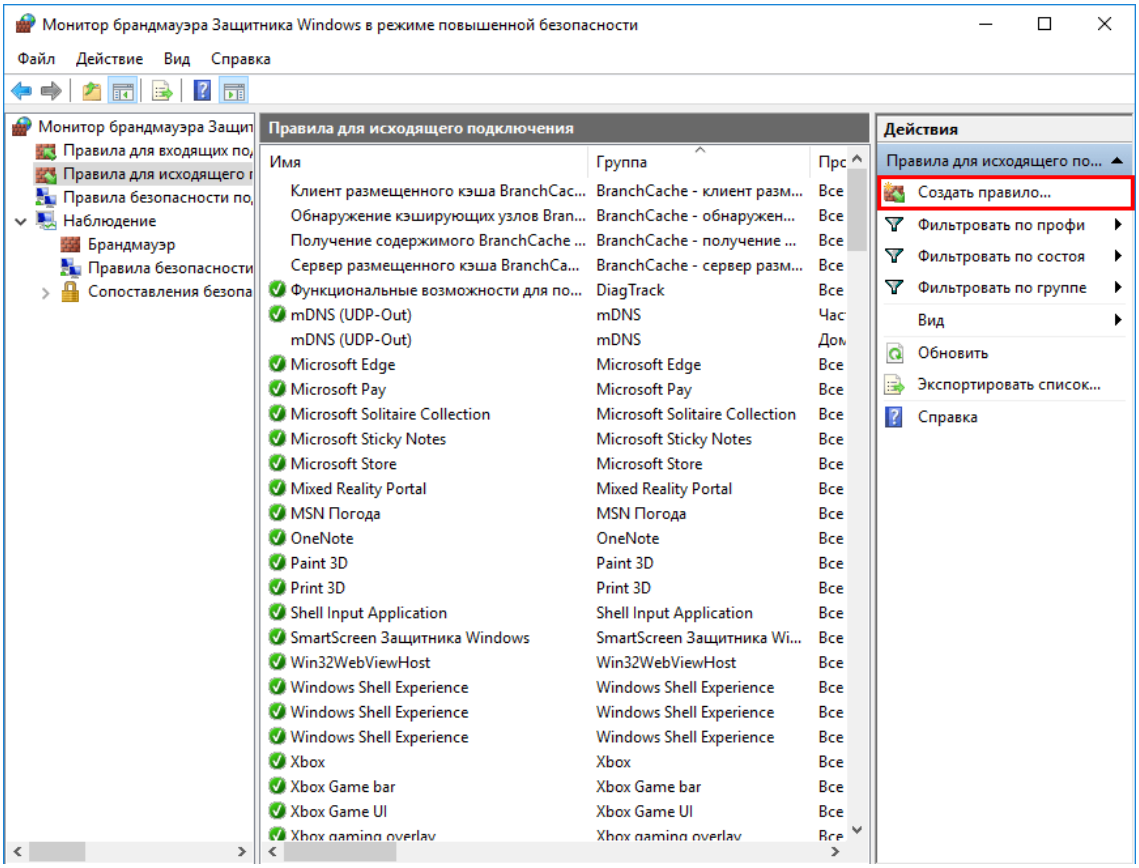

Рис. 34. Создание исходящего правила в МСЭ в Windows 10

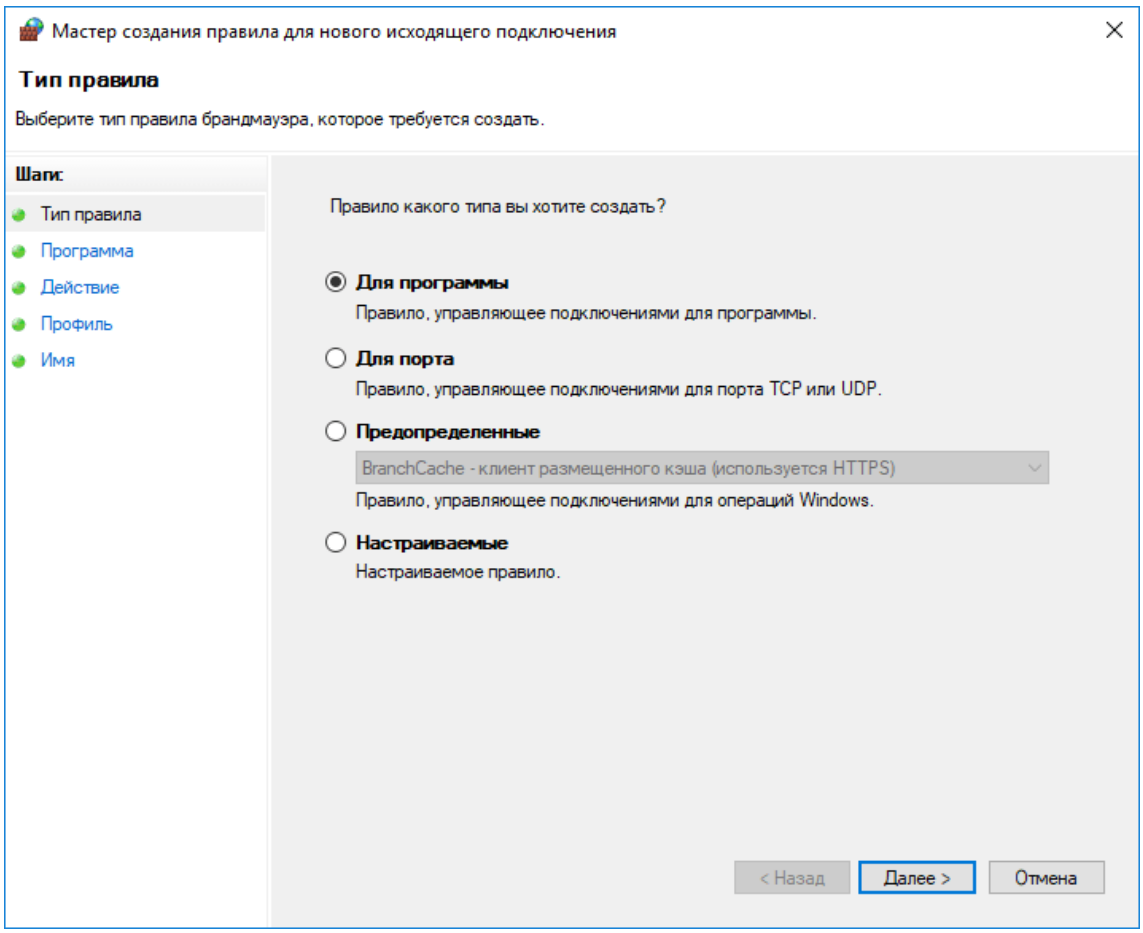

Рис. 35. Диалоговое окно «Мастер создания правила для нового исходящего подключения»

Выбираем «*Публичный*» (потому что хотим заблокировать доступ только тогда, когда компьютер подключен к общественной сети) и нажимаем «*Далее*» (рис. 38).

На шаге «*Имя*» введите имя, и описание для вновь созданного правила. Для завершения нажмите «*Готово*» (рис. 39).

Для создания входящего правила, перейдите к «*Правилам для входящих подключений*» и нажмите «*Создать правило*» в столбце справа (рис. 40).

Запустится «*Мастер создания правила для нового входящего подключения*».

В качестве примера создадим правило, которое блокирует весь входящий трафик, созданный с использованием протокола TCP на порте 30770.

На первом шаге «*Тип правила*» выберите значение «*Для порта*» (рис. 41).

На втором шаге «*Протокол и порты*» выберите протокол и порт, для которого применяется правило: протокол – TCP, порт – 30770 (рис. 42).

На третьем шаге «Действие» выберите значение «Блокировать подключение» и нажмите «Далее» (рис. 43).

На четвертом шаге «*Профиль*» необходимо сделать выбор профилей, для которых применяется правило. Поскольку предполагается блокировка всего TCP-трафик на порте 30770, выберите все три профиля и нажмите «*Далее*» (рис. 44).

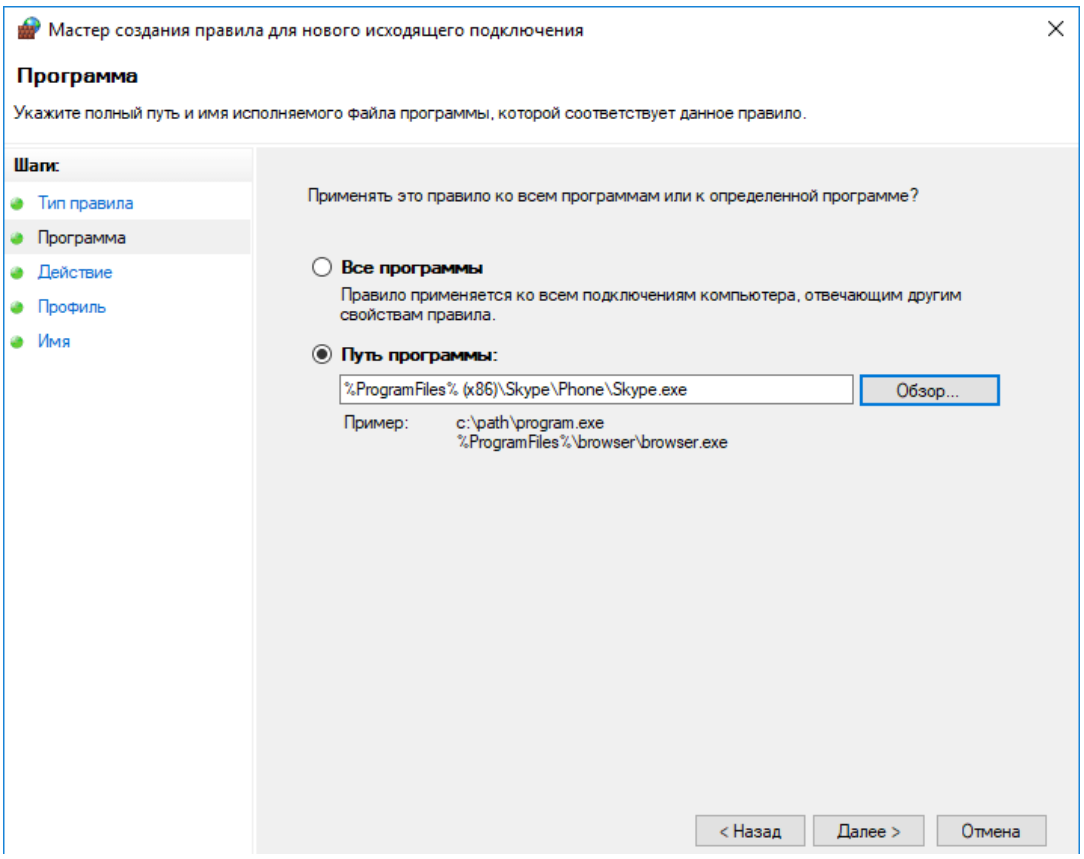

Рис. 36. Выбираем исполняемый файл программы, которую хотим заблокировать (Skype.exe) и переходим «Далее»

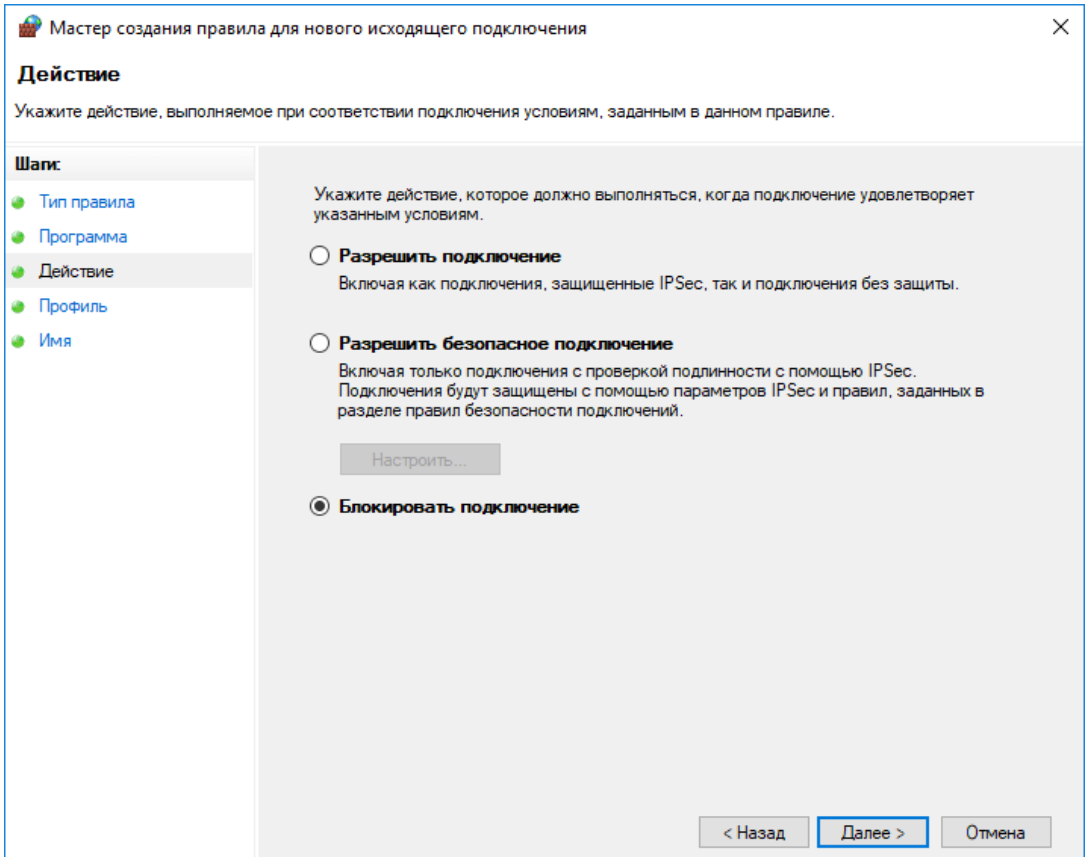

Рис. 37. Выбираем «Блокировать подключение» и нажимаем «Далее»

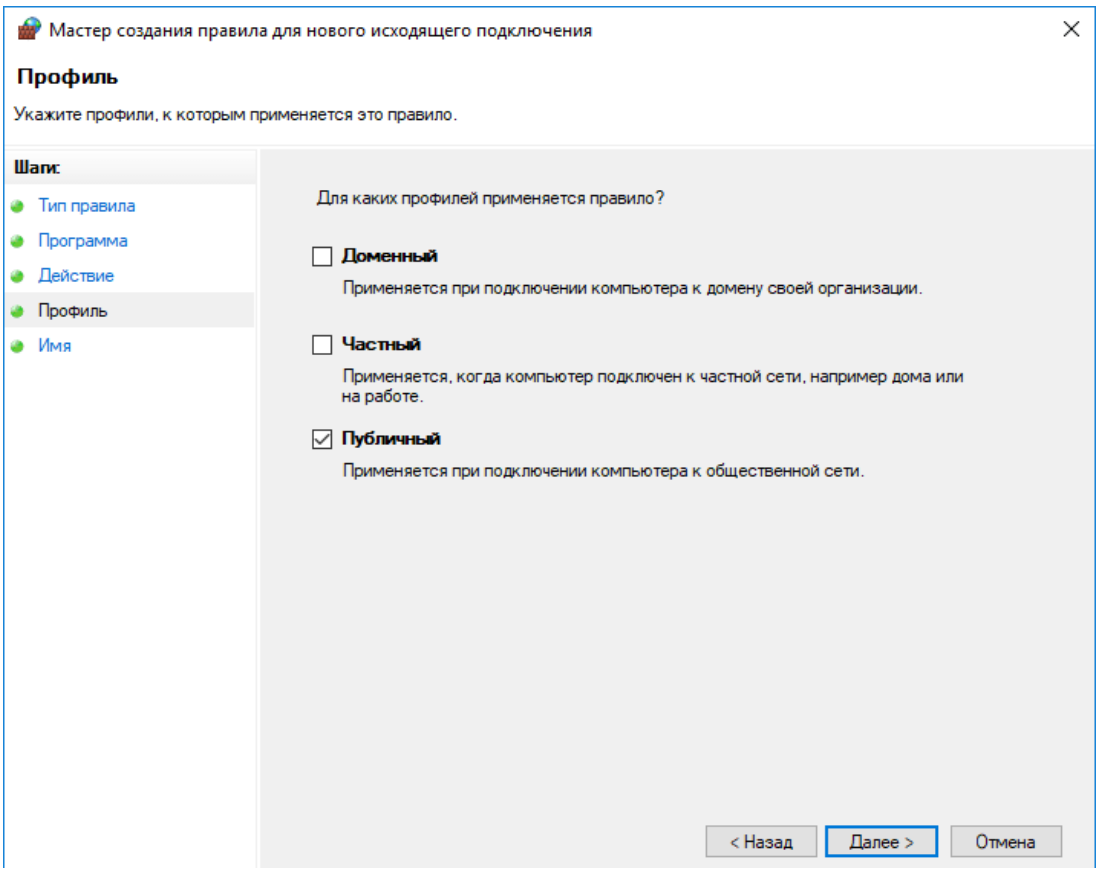

Рис. 38. Выбираем «Публичный» (потому что хотим заблокировать доступ только тогда, когда компьютер подключен к общественной сети) и нажимаем «Далее»

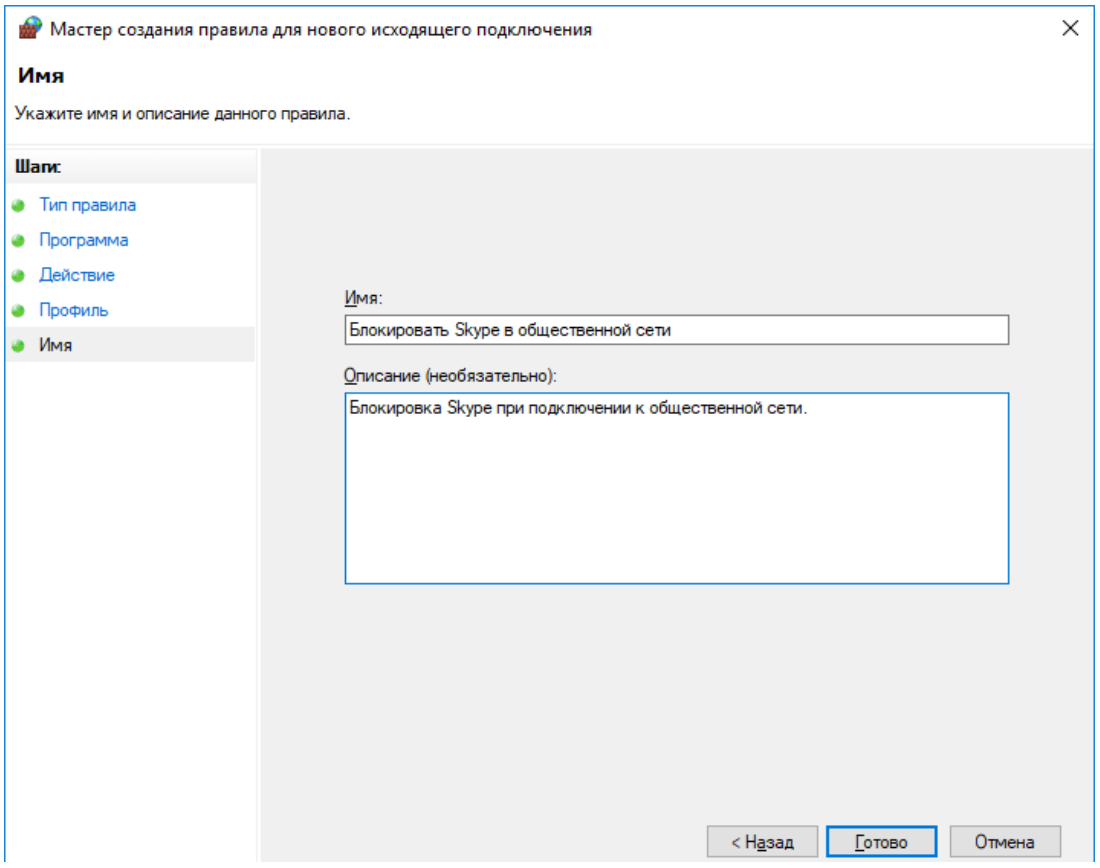

Рис. 39. На шаге «Имя» введите имя, и описание для вновь созданного правила.

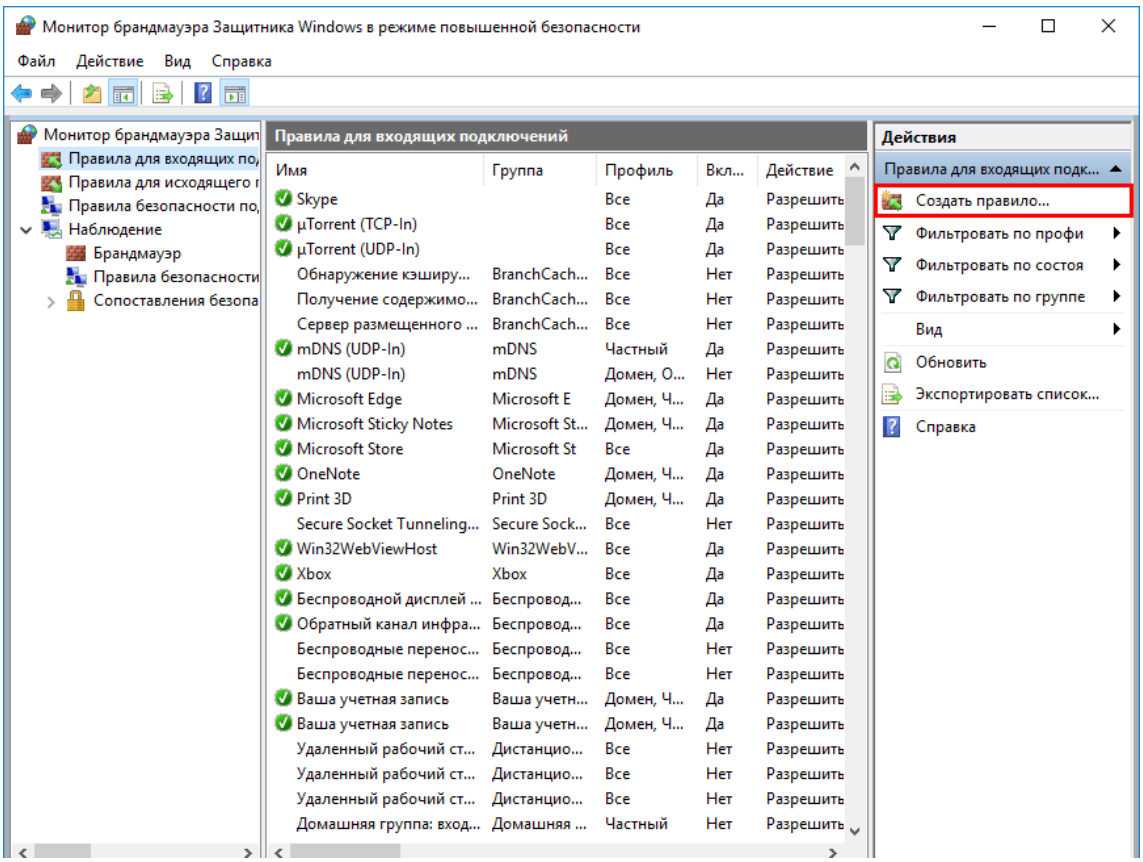

Рис. 40. Окно настроек в МСЭ в Windows 10

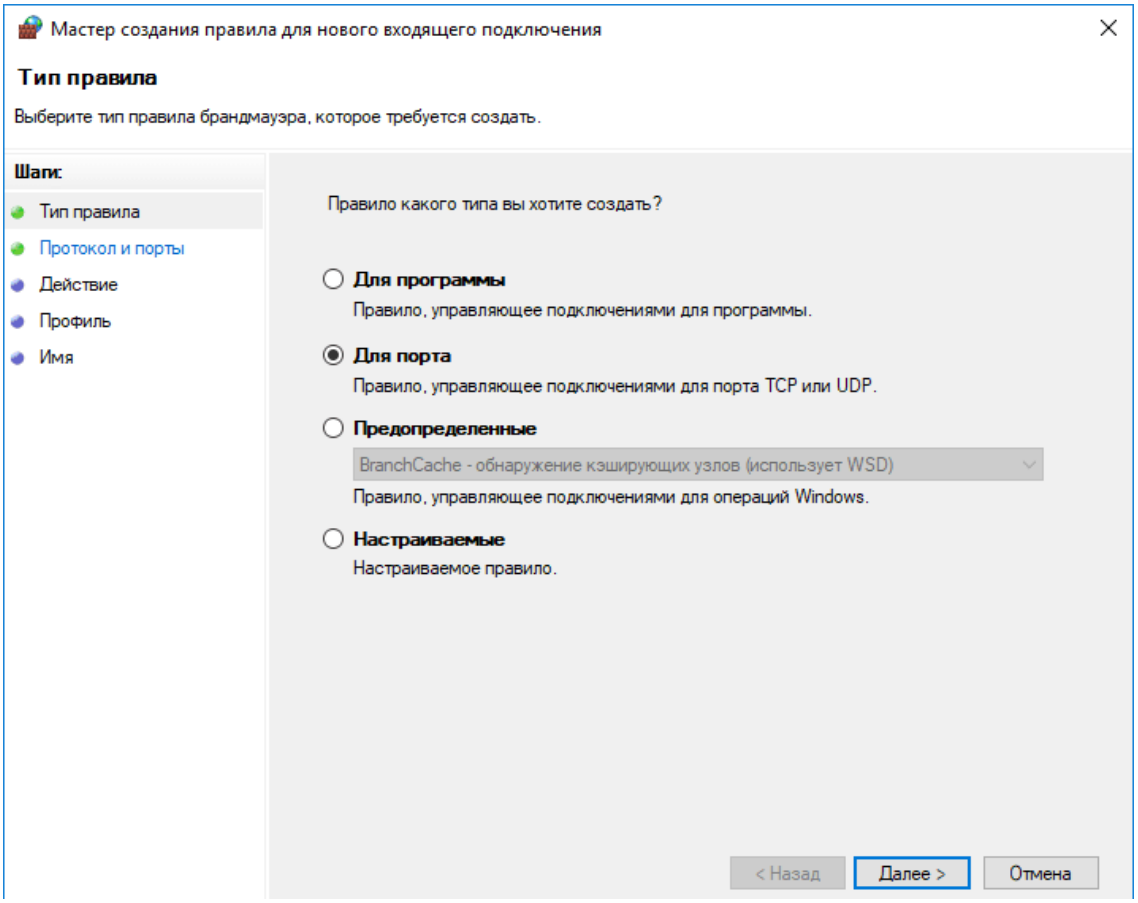

Рис. 41. Создание правила для нового входящего подключения в МСЭ

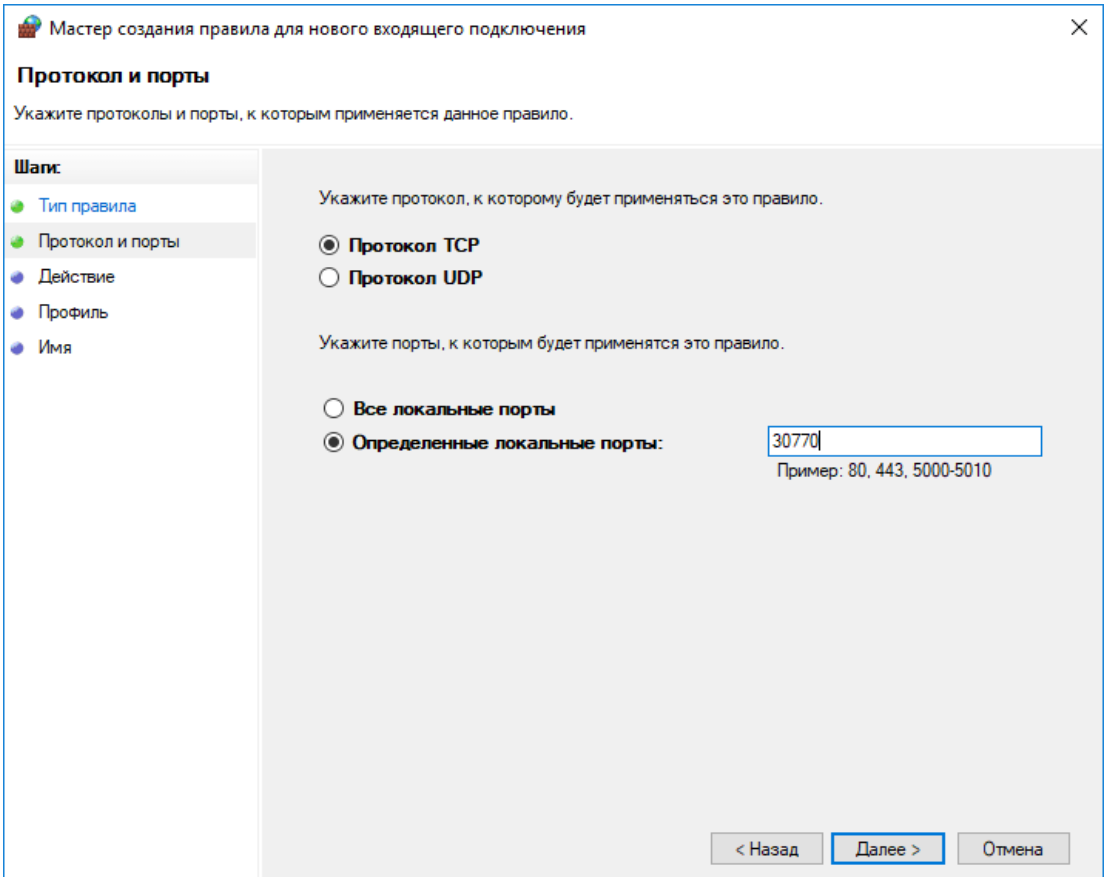

Рис. 42. Создание правила для нового входящего подключения в МСЭ

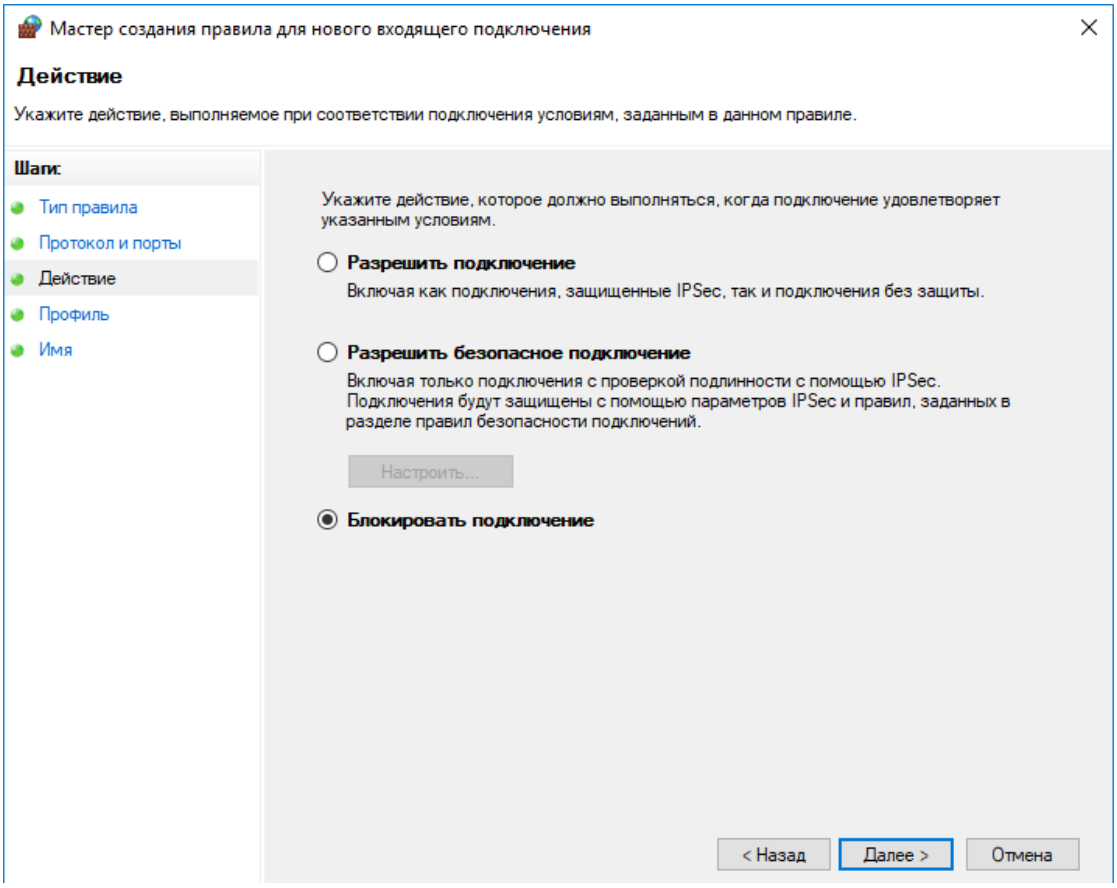

Рис. 43. Создание правила для нового входящего подключения в МСЭ

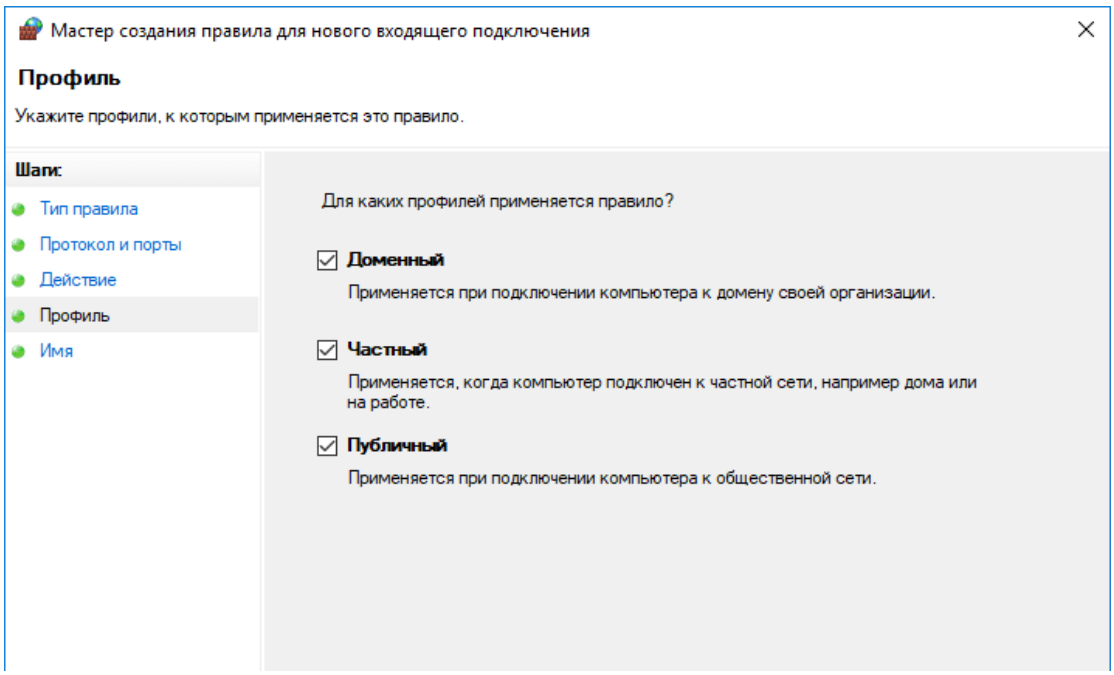

Рис. 44. Создание правила для нового входящего подключения в МСЭ

На заключительном этапе «Имя» введите имя и описание для вновь созданного правила., нажмите «Готово» (рис. 45).

Правило создано и теперь используется.

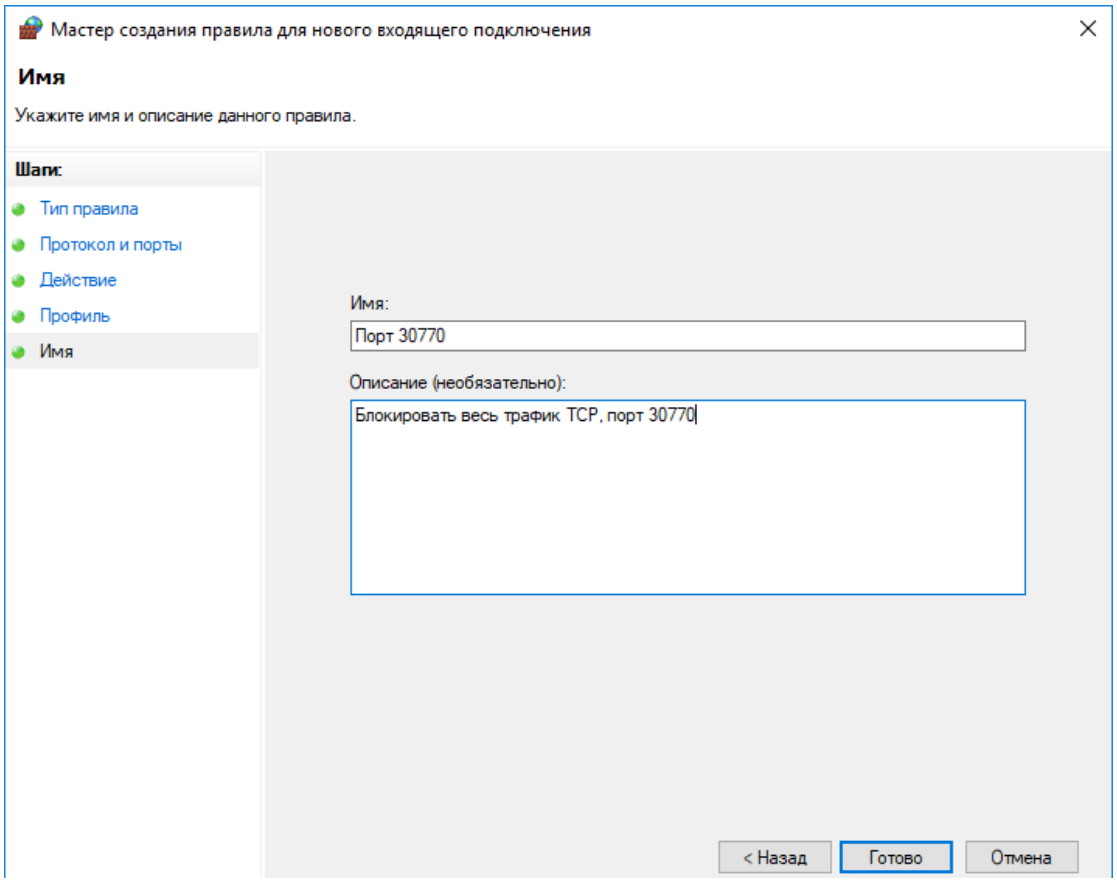

Рис. 45. Создание правила для нового входящего подключения в МСЭ

Восстановление параметров МСЭ по умолчанию

Для того, чтобы отменить все настройки МСЭ и вернуть их в состояние «По умолчанию», откройте брандмауэр Windows и в левом столбце, нажмите по ссылке «*Восстановить значения по умолчанию*» (рис. 46).

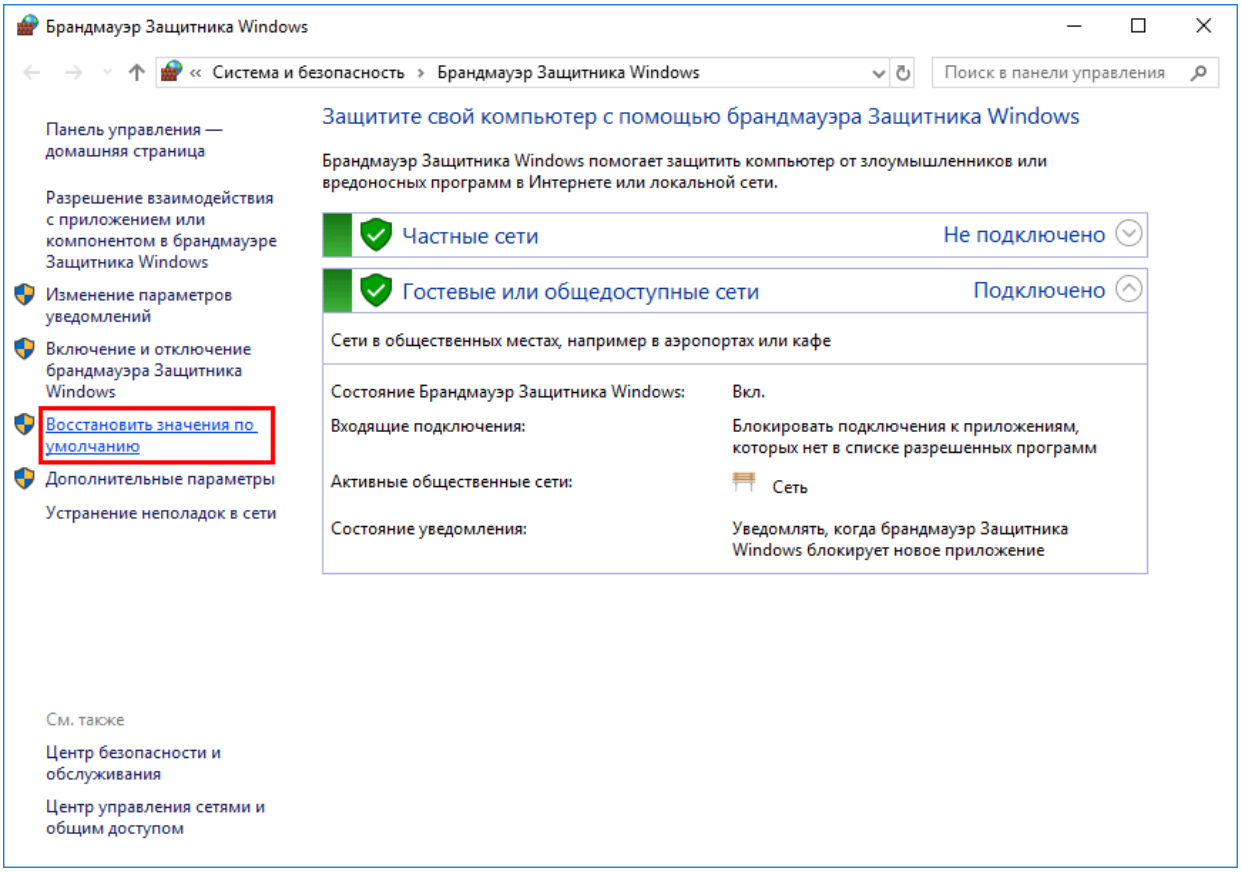

Рис. 46. Отмена настроек МСЭ в Windows 10

Нажмите на кнопку «*Восстановить значения по умолчанию*» (рис. 47).

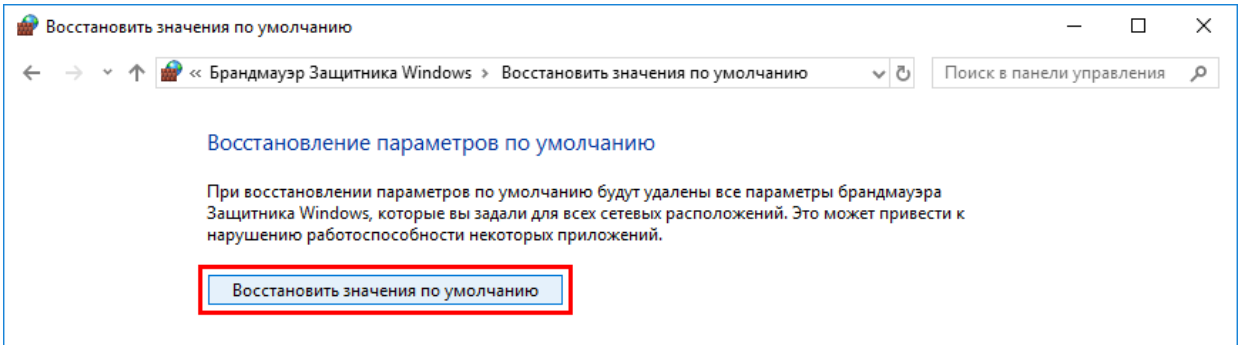

Рис. 47. Отмена настроек МСЭ в Windows 10

Подтвердите восстановление нажав на кнопку «Да» (рис. 48)
Параметры будут сброшены до значений по умолчанию.

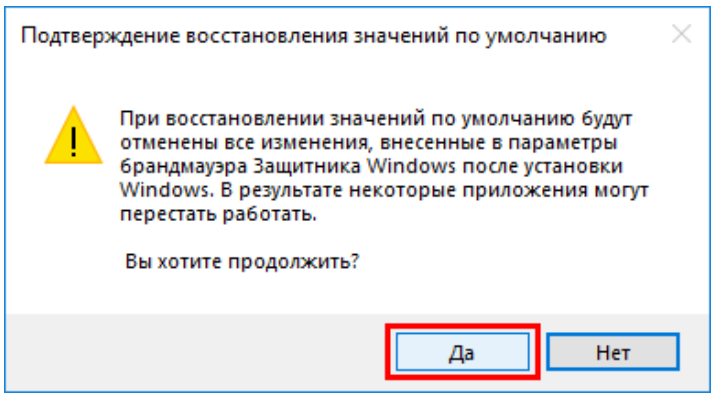

Рис. 48. Отмена настроек МСЭ в Windows 10

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Откройте МСЭ Windows. Удостоверьтесь в том, что брандмауэр включен для всех типов сетей. В противном случае выполните соответствующие подключения.

2. Осуществите в МСЭ просмотр сведений о том, какие одноранговые узлы подключены к вашему ПК и какой пакет защиты используется ОС для формирования сопоставлений безопасности. Найденную информацию зафиксируйте в файл-отчете.

2. Осуществите следующие настройте параметров МСЭ:

а) для *частной* сети: блокировать все входящие подключения – *нет*; уведомлять, когда МСЭ блокирует новое приложение – *да*;

б) для *общественной* сети: блокировать все входящие подключения – *нет*; уведомлять, когда МСЭ блокирует новое приложение – *да*.

4. С помощью МСЭ осуществите запрет доступа к частной сети для приложения «Windows Media Player».

5. Создайте исходящее правило в МСЭ, блокирующее доступ к сети Интернет для приложения «Total Commander» в случае подключения к общедоступным сетям.

6. В сети Интернет найдите информацию о наиболее уязвимых портах Windows 10. Используя полученную информацию, заполните в файле-отчете следующую таблицу:

Сведения об уязвимых портах Windows 10	
Протокол, номер порта	Описание

7. Создайте входящее правило в МСЭ, блокирующее входящий трафик, созданный с использованием протоколов на портах, указанных в вышеприведенной таблице.

8. Создайте входящее правило в МСЭ, блокирующее входящий TCP трафик с IP-адреса 37.45.250.150.

9. Продемонстрируйте результаты преподавателю.

10. Выполните сброс настроек МСЭ до уровня «*По умолчанию*».
11. Продемонстрируйте результаты преподавателю.
12. Удалите песочницу под именем «Гость1».
13. Подготовьте ответы на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Какие функции выполняет межсетевое экранирование?
2. Что такое режим повышенной безопасности в МСЭ?
3. Какие правила и исключения можно установить в МСЭ?

3. Создание образа системы

Краткие теоретические сведения:

Анализ практики раскрытия и расследования киберпреступлений свидетельствует о том, что в большинстве случаев в качестве доказательств по уголовным делам выступает информация, содержащаяся в электронных носителях информации, изымаемых в ходе проведения осмотров, выемок, обысков, других следственных действий и оперативно-розыскных мероприятий. Исследование таких электронных носителей предполагает создание точной побитовой копии для их дальнейшего изучения в лабораторных условиях.

Для того, чтобы создать точную побитовую копию носителя, следует воспользоваться специальным программным обеспечением, например: Acronis True Image. Данное программное обеспечение позволяет создавать образы (выполнять точное посекторное клонирование) носителей информации двумя способами:

с помощью загрузочного носителя (создается самостоятельно с помощью Acronis True Image);

с помощью программы Acronis True Image в ОС Windows (в этом случае исследуемый носитель информации должен быть подключен к служебному ПК с использованием средств, исключающих возможность записи на него).

Перед тем, как создавать образ системы, следует отметить, что исходный (клонируемый) и целевой (на который будет записан образ) диски должны иметь одинаковый размер логического сектора. Клонирование на диск с другим размером логического сектора не поддерживается.

Клонирование RAID-массивов поддерживается Acronis True Image только для простых систем разбиения диска, таких как MBR и GPT.

Аппаратные RAID-массивы могут быть клонированы при условии, что ОС, в которой работает продукт Acronis True Image, поддерживает их, поскольку Acronis True Image получает информацию о конфигурации RAID из ОС. При этом, клонирование аппаратного RAID будет работать только в том случае, если перезагрузка не требуется: после перезагрузки операция

продолжается в автономной версии Acronis True Image, где поддержка всех аппаратных конфигураций RAID не гарантируется и, следовательно, операция клонирования может завершиться неудачей после перезагрузки.

Рассмотрим некоторые особенности создания образов исследуемых носителей информации с помощью Acronis True Image в ОС Windows. Алгоритм реализации данной задачи (с учетом выполнения вышеуказанных условий) предполагает выполнение следующих действий.

1. Запустите программу Acronis True Image (2013). Откройте вкладку «*Резервное копирование и восстановление*». Нажмите на кнопку «*Резервное копирование дисков в разделов*» (рис. 56).

Откроется окно «*Резервное копирование дисков*» (рис. 57).

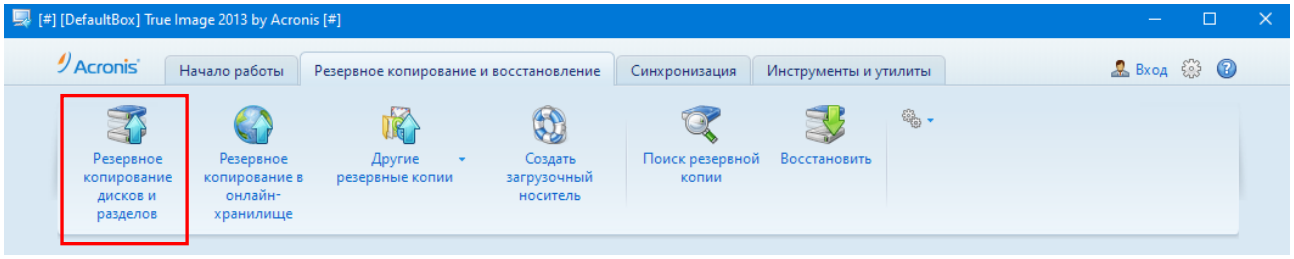

Рис. 56. Программа для резервного копирования данных и создания образов Acronis True Image (2013).

2. Нажмите на ссылку «*Переключиться в дисковый режим*» в правом верхнем углу (это нужно для того, чтобы создать образ всего диска, а не одного из его разделов), а затем установите флажок диска (носителя информации), образ которого будете создавать.

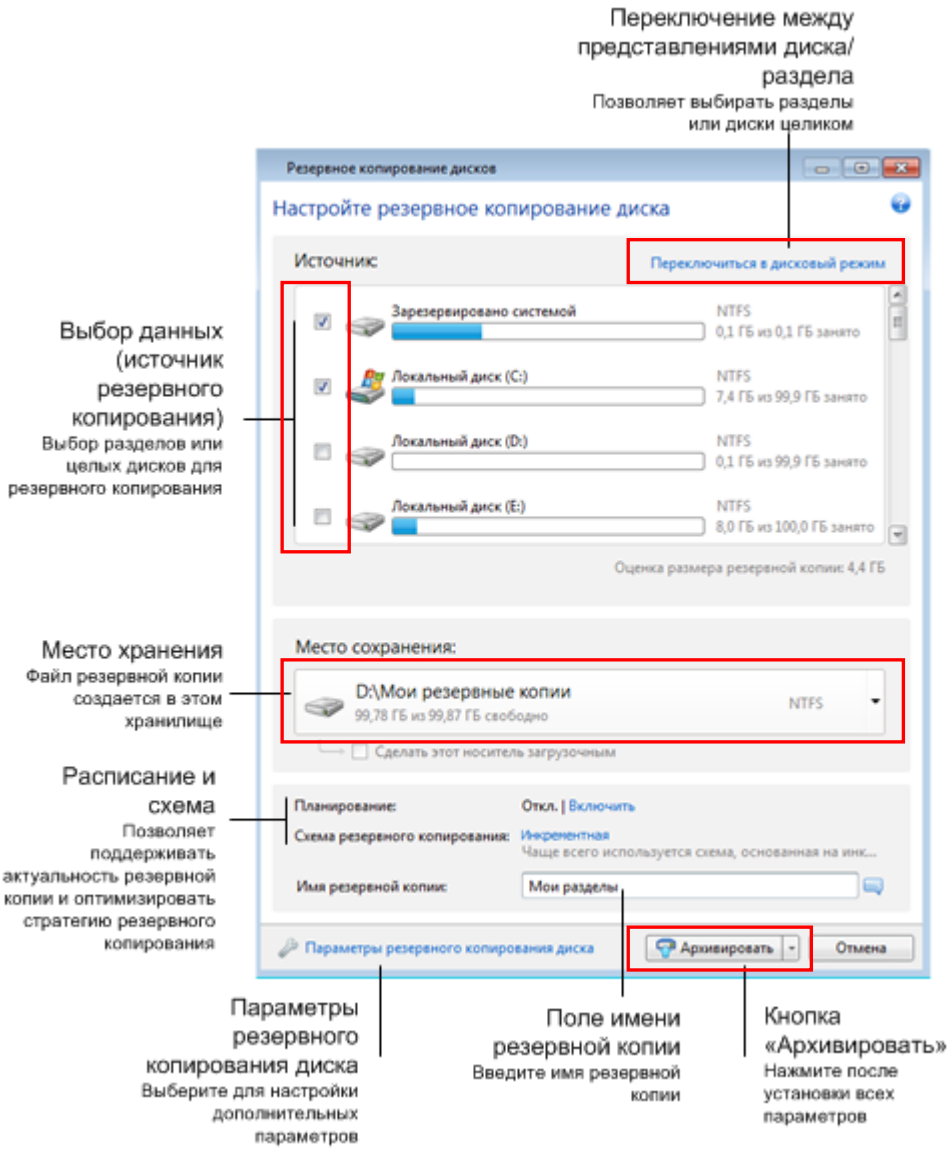

Рис. 57. Настройка параметров программы для резервного копирования данных и создания образов Acronis True Image (2013).

3. Выберите место сохранения образа (оставьте место сохранения «*По умолчанию*» или укажите другое, открыв параметр «*Место сохранения*» и выбрав пункт *Обзор*...).

4. Нажмите на ссылку «*Параметры резервного копирования диска*». Откроется соответствующее диалоговое окно (рис. 58).

Включите следующие параметры режима создания образа: «*Архивировать в посекторном режиме*» и «*Архивировать нераспределенное пространство*». Для продолжения нажмите кнопку «Ок». Окно «*Резервное копирование дисков*» закроется.

5. Чтобы завершить настройку параметров программы и перейти непосредственно к процессу создания образа нажмите на кнопку «*Архивировать*». Если необходимо запустить создание образа позже или в

соответствии с расписанием, откройте стрелку «Вниз» справа от кнопки «*Архивировать*» и выберите пункт «*Отложить*» в раскрывающемся списке.

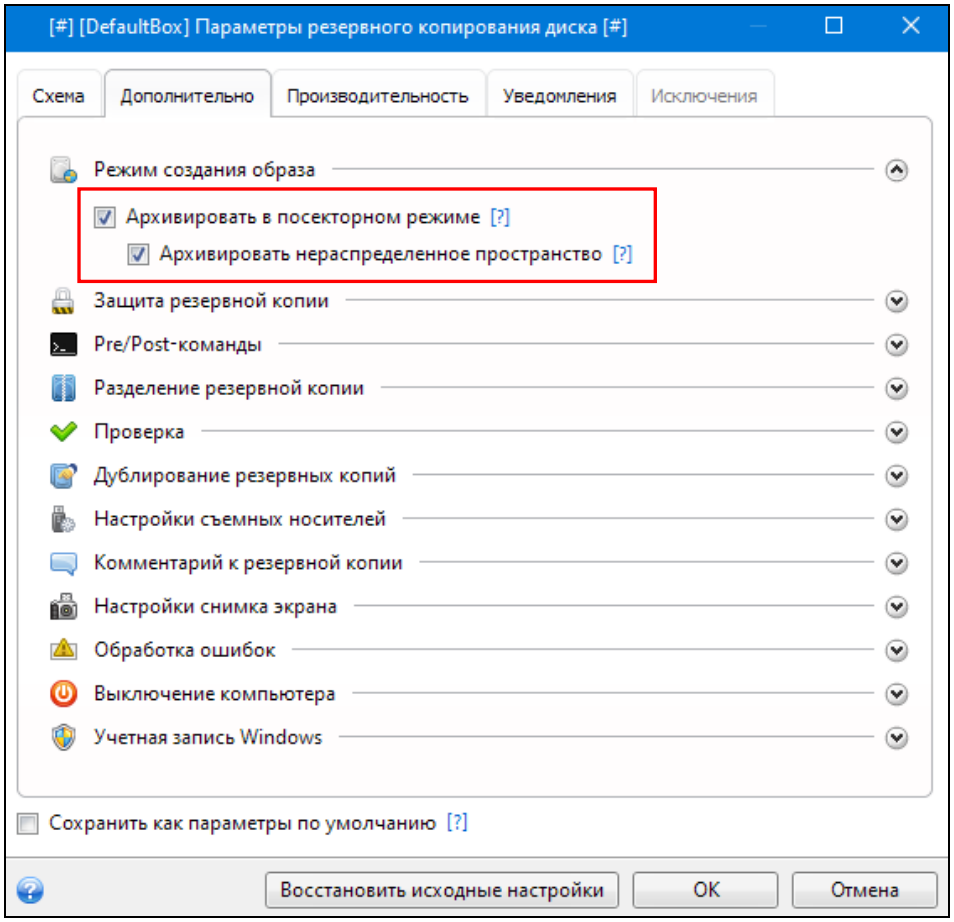

Рис. 58. Настройка параметров программы для резервного копирования данных и создания образов Acronis True Image (2013).

6. Когда создание образа завершится, вам будет предложено нажать любую клавишу, чтобы выключить компьютер. Завершите работу системы и только после этого удалите один из жестких дисков.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Запустите программу Acronis True Image (2013). Ознакомьтесь с пользовательским интерфейсом программы. Изучите особенности ее настройки в соответствии с вышеприведенными теоретическими сведениями.

2. Нажмите клавишу F1. Откроется окно справочной системы программы Acronis True Image. Самостоятельно изучите содержимое разделов «Приступая к работе», «Резервное копирование данных», «Инструменты и утилиты».

Откройте словарь терминов и ознакомьтесь с информацией о загрузочном носителе Acronis True Image. Зафиксируйте ее в файле-отчете.

3. Получите у преподавателя учебный USB-носитель и осуществите создание его образа (точной побитовой копии), сохранив его на диске D.

4. Продемонстрируйте результаты преподавателю.

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

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что означает понятие и что включает в себя «образ системы»? В каких случаях необходимо его создание? Приведите примеры.
2. Какие функции выполняет программа Acronis True Image?
3. Какие существуют способы создания образа системы с помощью программы Acronis True Image?
4. В каких случаях используется загрузочный носитель Acronis True Image?