Лабораторная работа № 2

**Защита от вредоносного ПО**

Цель работы: Изучить систему защиты от вредоносного программного обеспечения, ознакомиться с основными принципами управления архивации. Изучить основы блокировки трафика.

Операционные системы: Windows 8.1, Windows 10.

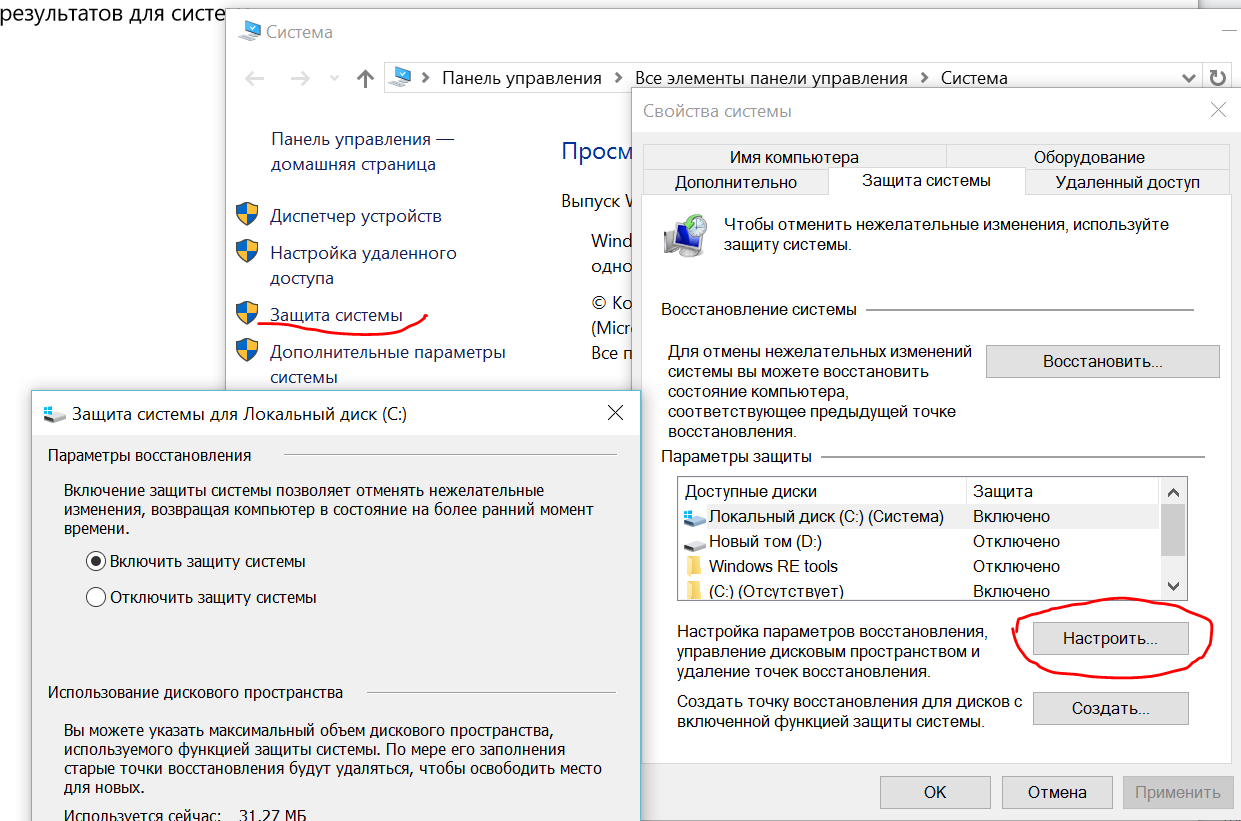
Краткий теоретический материал

Защита от вредоносного программного обеспечения – к этой категории относятся механизмы, обеспечивающие противодействие вредоносной активности программного обеспечения и позволяющие заблокировать доступ к критичной информации, перехвату управления и другим несанкционированным действиям. В этой же категории рассматриваются угрозы, направленные на автоматизированное распространение вредоносных программ и заражение других компьютеров. Актуальные угрозы в данной категории:

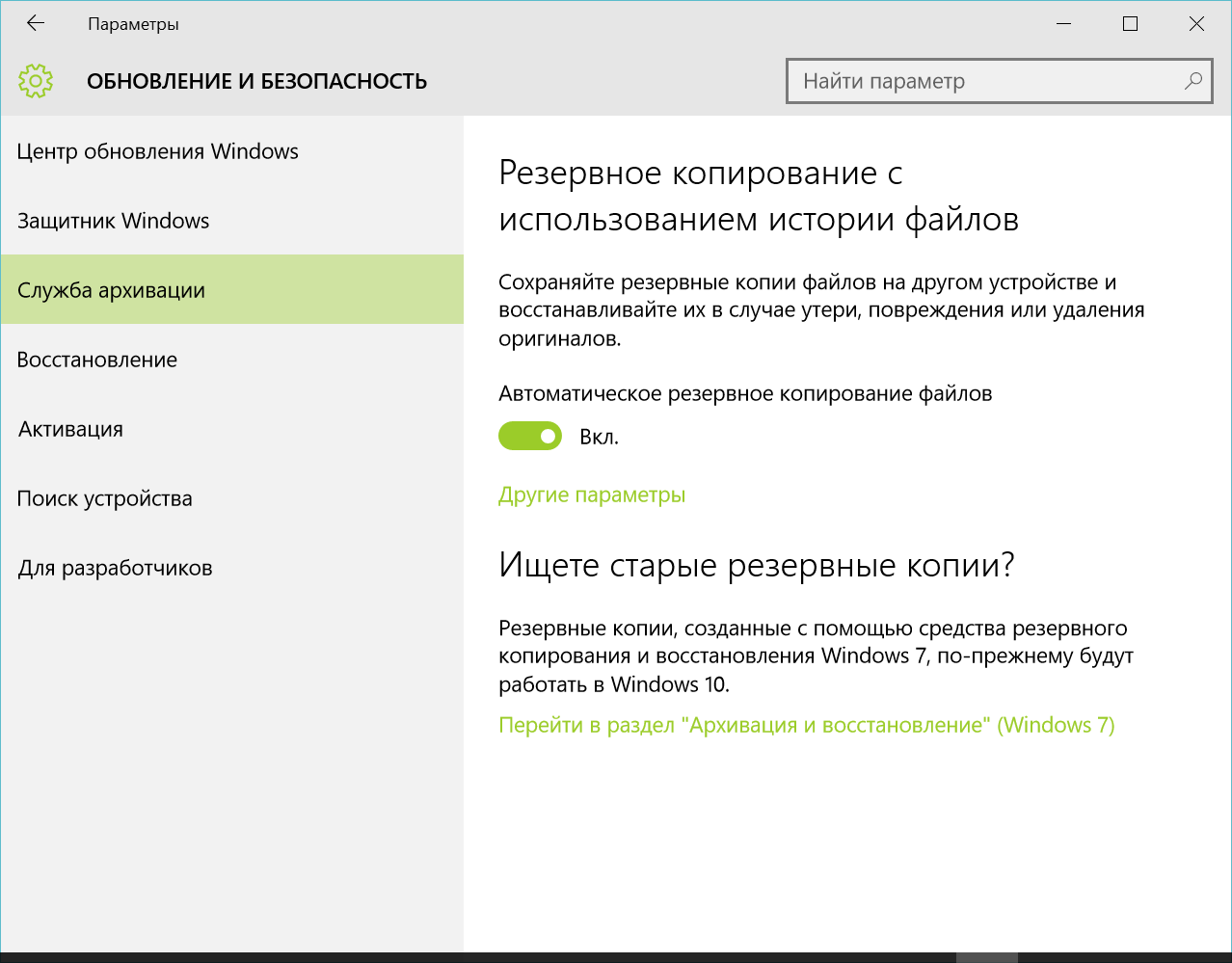
* 1. Заражение загрузочного сектора;
  2. Перехват паролей при входе в Windows и подмена экрана загрузки;
  3. Запуск вредоносного кода через эксплуатацию уязвимостей типа «переполнение буфера» в компонентах операционной системы и стороннего программного обеспечения;
  4. Вредоносное программное обеспечение, запускаемое пользователем;
  5. Перехват исполнения стандартных функций операционной системы;
  6. Вредоносное программное обеспечение, функционирующее как драйвер;
  7. Подмена служебных файлов и библиотек.

Для противодействия представленным угрозам в операционную систему уже встроены механизмы защиты. Многие из этих механизмов защиты работают автоматически и не нуждаются в настройках.

Для начала нам необходимо включить систему защиты. Необходимо перейти в панель управления, система и безопасность, система. Далее нужно выбрать нужный диск и нажать настройки, где будет предложено включить защиту системы.



Для сохранения системой предыдущих версий файлов в случае Windows 10 наберите в поиске «Параметры», выберите пункт «Обновление и безопасность», далее – «Служба архивации», – «Резервное копирование использованием истории файлов» (*Параметры – поиск -история файлов – служба архивации*). Можно не архивировать все подряд, меню «Другие параметры» позволяет выбрать конкретные папки, в которых лежат ваши важные файлы.



Один из популярнейших средств распространения вредоносного ПО это открытие пользователем исполняемого файла, который замаскирован под офисный документ (.doc, .xls, .pdf). В первую очередь необходимо включить «отображать расширение зарегистрированных типов файлов» и необходимо понять, что файлы с расширениями .exe, .js, .com, .pif,.cmd, .scr, .bat не могут быть офисными документами. Для включение отображения расширение, необходимо в поисковике Windows найти «параметры папок», вид и убрать галочку с пункта «Скрывать расширения для зарегистрированных типов файлов».

Весьма гибкие возможности контроля файлов предоставляют средства AppLocker или SRP в Windows, но эти функции присутствуют только в Enterprise- и Ultimate-редакциях операционной системы.

AppLocker — это функция операционных систем Windows, которая расширяет возможности управления приложениями и функциональность политик ограниченного использования программ. AppLocker включает возможности и расширения, позволяющие создавать правила разрешения и запрета выполнения приложений на основе уникальных удостоверений файлов, а также указывать пользователей или группы, которым разрешено запускать эти приложения.

С помощью AppLocker вы сможете выполнять следующие задачи.

* Управлять приложениями следующих типов: исполняемые файлы (с расширениями EXE и COM), сценарии (с расширениями JS, PS1, VBS, CMD и BAT), файлы установщика Windows (с расширениями MST, MSI и MSP), файлы библиотек DLL (с расширениями DLL и OCX), а также упакованные приложения и установщики упакованных приложений (с расширением APPX).
* Определять правила на основе атрибутов файлов, производных от цифровой подписи, включая издателя, название продукта, имя файла и версию файла. Например, можно создать правила на основе атрибута издателя, который сохраняется при всех обновлениях, или правила для конкретной версии файла.
* Назначить правило группе безопасности или отдельному пользователю.
* Создавать исключения для правил. Например, можно создать правило, разрешающее запуск всех процессов Windows, за исключением редактора реестра (Regedit.exe).
* Использовать режим "Только аудит" для развертывания политики и выяснения ее влияния перед применением.
* Импортировать и экспортировать правила. Импорт и экспорт затрагивают всю политику. Например, в случае экспорта политики экспортируются все правила из всех коллекций правил, включая параметры применения для коллекций правил. В случае импорта политики все условия существующей политики перезаписываются.
* Оптимизировать создание правил AppLocker и управление ими с помощью командлетов Windows PowerShell.

AppLocker позволяет упростить работу администраторов и снизить расходы на управление вычислительными ресурсами за счет уменьшения числа обращений в службу поддержки, возникающих вследствие запуска пользователями неутвержденных приложений.

Еще один способ заражения вредоносным ПО – это посещение подозрительных сайтов. Для снижения данного риска в операционной системе Windows имеется технология Smart Screen.

Smart Screen – комплексное решение по защите пользователя во время посещения веб - сайтов и других интернет - сервисов.

В состав Smart Screen входят три механизма: антифишинговая защита, проверка репутации загружаемых приложений и защита от загружаемых вредоносных программ.

# Smart Screen работает только в браузере Internet explorer и Microsoft Edge.

Функционал Smart Screen:

* С помощью механизма антифишинговой защиты, все сайты, которые пытается посетить пользователь, проверяются по специальной централизованной базе. Если на сайте были обнаружены поддельные формы авторизации, повторяющие формы различных сервисов (банки, магазины, платежные системы и т.д.), он заносится в общую базу. При попытке пользователя открыть такой сайт, доступ к нему блокируется с выводом предупреждения. Также под действие фильтра попадают сайты с известными вредоносными кодами и программным обеспечением.
* Репутационная проверка загружаемых файлов позволяет опознать файл после его загрузки и оценивает его опасность или безопасность для пользователя, основываясь на подписи файла, количестве его загрузок другими пользователями и попытками осуществить подозрительные и вредоносные действия на других компьютерах. Если файл признан не надежным, его запуск блокируется, пользователю выводятся специальные предупреждения о возможном вредоносном действии скачанного файла.
* Защита от вредоносных программ действует по принципу антифишинговой защиты – загруженные файлы проверяются по контрольным суммам в глобальной базе данных и, если файл в базе значится как вредоносный, пользователю выводится предупреждение, а запуск файла блокируется.
* Обновления браузера распространяются вместе с обновлениями операционной системы, поэтому пользователь при работе с вебсайтами максимально защищен и не рискует, заходя на незнакомую страницу, содержащую вредоносный код, даже если она еще не числиться в базе фишинга.

Для включения Smart Screen необходимо в поиске Windows вбить «безопасность и обслуживание». Далее вы увидите предложение о включение данной защиты.

Многие представители вредоносного ПО способны распространяться внутри сети. Для защиты от внешний атак и распространения вирусов в Windows был встроен Брандмауэр.

Брандмауэр Windows — встроенный в [Microsoft Windows](https://ru.wikipedia.org/wiki/Microsoft_Windows" \o "Microsoft Windows) [межсетевой экран](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD). Появился в [Windows XP](https://ru.wikipedia.org/wiki/Windows_XP" \o "Windows XP) SP2. Одним из отличий от предшественника (Internet Connection Firewall) является контроль доступа программ в сеть. Брандмауэр Windows является частью [Центра обеспечения безопасности](https://ru.wikipedia.org/wiki/Windows_Security_Center) Windows.

Встроенный брандмауэр кроме стандартной фильтрации входящего трафика, появились функции управления исходящим трафиком, активный мониторинг текущего трафика, а также встроенное управление правилами безопасности подключений IPSec и многие другие функции.

(http://windows.microsoft.com/ru-ru/windows-8/windows-firewall-from-start-to-finish)

Рекомендуется использовать следующие параметры брандмауэра по умолчанию.

* Брандмауэр включен для всех сетевых подключений.
* Брандмауэр блокирует все входящие подключения, кроме явно разрешенных пользователем.
* Брандмауэр включен для всех типов сетей (частные, публичные и доменные).

## Включение и отключение брандмауэра Windows

Брандмауэр Windows не следует отключать, пока не включен другой брандмауэр. Отключение брандмауэра Windows может повысить уязвимость компьютера (и сети) к червям и злоумышленникам.

1. Откройте брандмауэр Windows. Для этого поместите курсор в правый верхний угол экрана, затем переместите его вниз и щелкните **Поиск**. После этого в поле поиска введите **брандмауэр**, а затем выберите элемент **БрандмауэрWindows**.
2. Выберите пункт **Включение и отключение брандмауэра Windows**. Вам может потребоваться ввести пароль учетной записи администратора или подтвердить выбор.
3. Выполните одно из указанных ниже действий.
   * Щелкните или коснитесь **Включить брандмауэр Windows**для каждого типа сети, в котором нужно включить защиту, а затем нажмите **ОК**.
   * Щелкните или коснитесь **Отключить брандмауэр Windows (не рекомендуется)**для каждого типа сети, в котором нужно отключить защиту, а затем нажмите **ОК**.

## Общие сведения о параметрах брандмауэра Windows

Для каждого типа сети (публичные, частные, доменные) можно настроить четыре параметра.

* **Включить брандмауэр Windows**. Эта настройка выбрана по умолчанию. Когда брандмауэр Windows включен, большинство приложений не могут получать данные через брандмауэр. Чтобы разрешить приложению получение данных, добавьте его в список разрешенных, как описано в следующем разделе. В частности, вы не сможете получать фотографии через приложение передачи мгновенных сообщений, пока это приложение не будет добавлено в список разрешенных.
* **Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ**. Этот параметр блокирует все неожидаемые попытки подключения к компьютеру. Используйте его, чтобы обеспечить максимальную защиту компьютера, например при подключении к публичной сети в гостинице или в аэропорту. При блокировке всех входящих подключений можно просматривать большинство веб-страниц, отправлять и принимать электронную почту, а также отправлять и принимать мгновенные сообщения.
* **Уведомлять, когда брандмауэр Windows блокирует новое приложение**. Если установлен этот флажок, то брандмауэр Windows уведомляет пользователя о блокировке нового приложения и дает возможность отменить блокировку.
* **Отключить брандмауэр Windows (не рекомендуется)**. Не выбирайте этот параметр, если на компьютере не работает другое приложение брандмауэра.

## Разрешение получения данных через брандмауэр для приложения

По умолчанию брандмауэр Windows блокирует большинство приложений, чтобы повысить безопасность компьютера. Для полноценной работы некоторых приложений может потребоваться получение данных через брандмауэр.

Прежде чем разрешать приложению получать данные через брандмауэр, необходимо оценить все риски, связанные с таким подключением

1. Откройте брандмауэр Windows.
2. Щелкните **Разрешение взаимодействия с приложением или компонентом в брандмауэре Windows**.
3. Нажмите кнопку **Изменить параметры**. Требуется разрешение администратора Вам может потребоваться ввести пароль учетной записи администратора или подтвердить выбор.
4. Установите флажок рядом с приложением, которое следует разрешить, выберите типы сетей, в которых вы хотите разрешить обмен данными, и нажмите **ОК**.

## Открытие порта в брандмауэре Windows

Если брандмауэр Windows блокирует приложение, а вы хотите разрешить этому приложению получение данных через брандмауэр, то для этого нужно выбрать приложение в списке разрешенных, как описано в предыдущем разделе.

Если приложение отсутствует в списке, то может понадобиться открыть порт (приложения получают данные через брандмауэр посредством портов). Например, чтобы играть с друзьями в многопользовательскую игру по Интернету, необходимо открыть порт для этой игры так, чтобы брандмауэр разрешал передачу ее данных на компьютер. Порт остается открытым постоянно, поэтому закрывайте порты, если они больше не требуются.

1. Откройте брандмауэр Windows.
2. Выберите пункт **Дополнительные параметры**.  Вам может потребоваться ввести пароль учетной записи администратора или подтвердить выбор.
3. В левой части диалогового окна **Брандмауэр Windows в режиме повышенной безопасности** выберите ссылку**Правила для входящих подключений**, а затем в правой части окна нажмите кнопку **Создать правило**.
4. Следуйте инструкциям на экране.

Задание

<http://remontka.pro/razbit-hdd/> - разметить диск.

<http://www.securitylab.ru/blog/company/hlsec/265329.php> (помощь 1-3 пункты)

1. Включить защиту системы Windows (*Путь: панель управления / система и безопасность / система. Включить защиту системы. Выбрать диск – настройки включить защиту системы*)
2. Включить отображение расширений
3. Настроить архивацию истории файлов. Создать 2 тестовых файлов. Записать в них одинаковый текст. ( *Параметры-поиск-история файлов – служба архивации*)
   1. Включить архивацию истории
   2. Внести в 1 из файлов в исключение
   3. Изменить время сохранение истории
   4. Изменить время хранение истории
   5. Внести изменения в оба файла
   6. Продемонстрировать историю файлов
   7. Откатить один из файлов
   8. Создать резервную копию образа системы
4. Включить SmartScrean и настроить его на отображение предупреждений.(поиск: безопасность и обслуживание)
5. Включить AppLocker и запретить пользователям студентам, открывать программу Regedit.exe. А гостю запретить запуск всех программ, кроме internet explore.

( [*https://www.youtube.com/watch?v=uIrQbh4Tv00*](https://www.youtube.com/watch?v=uIrQbh4Tv00))

1. Настроить Брадмауэр (Локальная политика безопасности)
   1. Создать исходящее правило. Запретить программу internet explore
   2. Создать входящее правило. Заблокировать порт (любой на ваше усмотрение, продемонстрировать запрет с помощью 2-ой машины)

**Отчет необходимо оформить по шаблону с сайта «ЛЭТИ» (титульник, цель работы, ход выполнения работы, вывод) и сопроводить скриншотами с этапами выполнения задания.**

**Отчеты присылать на почту** [ZOC.leti@yandex.ru](https://vk.com/write?email=ZOC.leti@yandex.ru) **. В теме письма должно содержаться имя, фамилия, группа, номер лабораторной работы и слово «Windows».**