МИНОБРАНАУКИ РОССИИ

Санкт-Петербургский государственный электротехнический

университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

**ЗАЩИТА ОПЕРАЦИОННЫХ СИСТЕМ И СИСТЕМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ**

Лабораторный практикум

Санкт-Петербург

СПбГЭТУ «ЛЭТИ»

2016

Авторы: **А. А. Молдовян, А. Н. Березин, И. В. Ковалева**

Защита операционных систем и систем управления базами данных: лабораторный практикум. СПбГЭТУ «ЛЭТИ», 2017. 48 с.

Содержит описание лабораторных работ и краткие теоретические сведения о средствах защиты операционных систем Windows и Linux.

Предназначены для студентов специальности 10.05.01, также могут быть полезны преподавателям и специалистам в области защиты информации.

Одобрено

Методической комиссией факультета

компьютерных технологий и информатики

в качестве учебно-методического пособия

©СПбГЭТУ «ЛЭТИ», 2016

Оглавление

[ВВЕДЕНИЕ 6](#_Toc482801713)

[1. СРЕДСТВА ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS 8](#_Toc482801714)

[1.1. Исследование средств обеспечения безопасности учетных записей и разграничения доступа 8](#_Toc482801715)

[Цель работы. 8](#_Toc482801716)

[Поддерживаемые операционные системы. 8](#_Toc482801717)

[Теоретические сведения. 8](#_Toc482801718)

[Постановка задачи. 14](#_Toc482801719)

[Последовательность действий. 14](#_Toc482801720)

[1.2. Исследование средств защиты от вредоносного ПО 15](#_Toc482801721)

[Цель работы. 15](#_Toc482801722)

[Поддерживаемые операционные системы. 15](#_Toc482801723)

[Теоретические сведения. 15](#_Toc482801724)

[Постановка задачи. 22](#_Toc482801725)

[Последовательность действий. 22](#_Toc482801726)

[1.3. Исследование средств отражения внешних атак 23](#_Toc482801727)

[Цель работы. 23](#_Toc482801728)

[Поддерживаемые операционные системы. 23](#_Toc482801729)

[Теоретические сведения. 23](#_Toc482801730)

[Постановка задачи. 28](#_Toc482801731)

[Последовательность действий. 29](#_Toc482801732)

[2. СРЕДСТВА ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX 30](#_Toc482801733)

[2.1. Создание базовой конфигурации 30](#_Toc482801734)

[Цель работы. 30](#_Toc482801735)

[Поддерживаемые операционные системы. 30](#_Toc482801736)

[Теоретические сведения. 31](#_Toc482801737)

[Постановка задачи. 35](#_Toc482801738)

[Последовательность действий. 36](#_Toc482801739)

[2.2. Изучение подсистемы безопасности в ОС Linux 36](#_Toc482801740)

[Цель работы. 36](#_Toc482801741)

[Поддерживаемые операционные системы. 36](#_Toc482801742)

[Теоретические сведения. 36](#_Toc482801743)

[Постановка задачи. 45](#_Toc482801744)

[Последовательность действий. 45](#_Toc482801745)

[СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ 47](#_Toc482801746)

# ВВЕДЕНИЕ

Предлагаемые темы для выполнения лабораторных работ направлены на закрепление материала и получение практических навыков, относящегося к защите операционных систем. Для выполнения данных лабораторных работ потребуется установка одной из предложенных операционных систем и ее настройка в соответствии с требованиями конкретного задания. Для удобства работы и простоты устранения возможных проблем необходимая операционная система может быть установлена на виртуальную машину, а не в качестве основной операционной системы пользователя.

Данный практикум направлен на изучение механизмов безопасности, принципов построения защиты информации и анализа надежности защиты в современных ОС. Кроме того, он формирует у обучаемых знания в области теоретических основ информационной безопасности и умений практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Лабораторный практикум состоит из двух разделов: средства защиты операционной системы Windows и средства защиты операционной системы Linux.

Настоящий лабораторный практикум включает следующие лабораторные работы:

1. Исследование средств обеспечения безопасности учетных записей и разграничения доступа в ОС Windows.
2. Исследование средств защиты от вредоносного ПО в ОС Windows.
3. Исследование средств отражения внешних атак в ОС Windows.
4. Создание базовой конфигурации в ОС Linux.
5. Изучение подсистемы безопасности в ОС Linux.

При выполнении заданий на практических целесообразно акцентировать внимание слушателей на используемых средствах защиты и нюансах их установки и работы. Заслуживают пояснения и некоторые частные аспекты. Например, в лабораторной работе «Исследование средств отражения внешних атак» важно сделать снимки текущего состояния виртуальной машины перед внесением изменений. Кроме того, в этой же лабораторной работе могут возникнуть трудности при попытке зашифровки носителя с помощью технологии BitLocker, которые также стоит обговорить заранее. При выполнении лабораторной работы по изучению подсистемы безопасности в ОС Linux целесообразно упомянуть о наличии man руководств, более подробно описывающих некоторые утилиты и функции, а также уточнить, где именно с ними можно ознакомиться.

Описание каждой лабораторной работы включает: название, цель работы, список поддерживаемых операционных систем, теоретические сведения, постановку задачи и последовательность действий исполнителя.

Предполагается, что обучающиеся к моменту начала выполнения учебных задач прослушали курсы «Основы информационной безопасности», «Операционные системы», «Архитектура информационных систем», «Криптографические методы защиты информации» и «Криптографические протоколы», а также приступили к ознакомлению с курсом «Администрирование защищенных информационных систем».

Отчет по каждой лабораторной должен содержать:

1. Титульный лист.
2. Цель работы.
3. Описание выполнения представленной в работе последовательности действий, включающее в себя как комментарии исполнителя, так и скриншоты, подтверждающие выполнение поставленных задач.
4. Вывод по выполненной работе.
5. Список использованной литературы.

# СРЕДСТВА ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS

## Исследование средств обеспечения безопасности учетных записей и разграничения доступа

Цель работы.Целью лабораторной работы является изучение типов учетных записей пользователей и основ разграничения доступа пользователей, а также ознакомление с основными принципами управления учетными записями.

Поддерживаемые операционные системы.Windows 7, Windows 8.1, Windows 10.

Теоретические сведения. Учетная запись пользователя определяет схему взаимодействия пользователя с компьютером и персонализирует ее. Например, учетная запись пользователя определяет к каким приложениям, папкам и файлам у вас есть доступ, какие изменения вы можете вносить в работу компьютера, а также задает персональные настройки, такие как макет начального экрана, фон рабочего стола и заставка. При создании отдельных учетных записей для разных пользователей не обязательно дублировать параметры для них. Это означает, что вы можете ограничить доступ к папке входящих писем, социальным сетям и другим файлам, а также устанавливать различные цвета и фоны рабочего стола для разных учетных записей.

Учетная запись в операционной системе Windows – это не что иное, как способ идентификации пользователей, благодаря чему операционная система может применять конкретные параметры для каждого пользователя.

В операционных системах Windows тип учетной записи пользователя определяет, какие задачи может выполнять на компьютере пользователь, в некоторых случаях могут потребоваться права администратора для выполнения некоторых задач или для использования некоторых приложений. Ниже описаны три типа учетных записей на компьютере с системой Windows:

1. Учетные записи обычных пользователей предназначены для повседневной работы.
2. Учетные записи администратора предоставляют полный контроль над компьютером и должна использоваться только при необходимости.
3. Учетные записи гостя предназначены для временного доступа на компьютер.

По способу авторизации можно выделить две группы:

1. локальная учетная запись;
2. сетевая учетная запись, для авторизации под которой нужно соединяться с удаленным сервером Microsoft.

Особенностью сетевых записей является то, что именно используя их, Вы получаете все возможности новой операционной системы, а также доступ ко всем сервисам. Единственная проблема этих записей: если не будет соединения с сервером авторизации Microsoft, то вход в компьютер не будет выполнен. Что касается локальных записей, то они ограничены по доступу к сетевым службам системы, но для полноценной работы более чем самодостаточны.

Существует несколько способов создания учетных записей:

1. Создание учетных записей пользователей для компьютеров, состоящих в рабочей группе:
   1. Создание учетной записи при помощи диалога «Управление учетными записями пользователей».
   2. Создание учетной записи при помощи диалога «Учетные записи пользователей».
   3. Создание учетной записи при помощи оснастки «Локальные пользователи и группы».
   4. Создание учетной записи при помощи командной строки (команда net user).
2. Создание учетных записей пользователей для компьютеров, состоящих в домене:
   1. Создание пользователей при помощи оснастки «Active Directory – пользователи и компьютеры».
   2. Создание пользователей с помощью командной строки (команда dsadd user).
   3. Импорт пользователей с помощью команды CSVDE.
   4. Импорт пользователей с помощью команды LDIFDE.
   5. Создание пользователей с помощью Windows PowerShell.
   6. Создание пользователей с помощью VBScript.

Для того чтобы произвести изменения в учетных записях, Вы должны обладать правами администратора, так как именно наличие этих прав и даст возможность проводить манипуляции с учетной записью. Сразу следует отметить, что нельзя удалить единственного администратора, а также перевести его в разряд пользователей, так как это приведет к неуправляемости компьютером. Администратор может управлять любой учетной записью, даже не имея пароля к ней.

Для того чтобы сменить тип учетной записи, нужно открыть «Панель управления», переключить режим отображения в «Категория» после чего выбрать раздел «Учетная запись». После этого стоит перейти по ссылке «Изменение типа учетной записи». Далее нужно выбрать нужную учетную запись и изменить ее тип, использовав появившееся меню. Далее выбрать роль учетной записи (администратор или обычный пользователь).

Изменение пароля выполняется также из панели управления, далее «Учетная запись», затем «Изменение типа учетной записи» (это поможет отобразить сразу всех пользователей). Выбираем нужного пользователя, после чего изменяем нужные данные. Пароль меняется администратором без сохранения предыдущего. Чтобы изменить имя или пароль следует воспользоваться пунктами меню. После чего подтвердить изменения, нажав на кнопку. Имя пользователя изменяется аналогичным образом.

Файловая система(file system) – способ организации данных в виде файлов на устройствах внешней памяти (жестких и оптических дисках, устройствах флеш-памяти и т. п.). Файловая система представляет собой иерархическое хранилище пользовательских и системных файлов, а также областей данных. В операционных системах существует большое количество файловых систем.

Windows поддерживает несколько файловых систем для различных внешних устройств:

1. NTFS – основная файловая система семейства Windows NT;
2. FAT (File Allocation Table – таблица размещения файлов) – простая файловая система используемая Windows для устройств флеш-памяти, а также для совместимости с другими операционными системами при установке на диски с множественной загрузкой. Основным элементом этой файловой системы является таблица размещения файлов FAT (по имени которой названа вся файловая система), необходимая для определения расположения файла на диске. Существует три варианта FAT, отличающихся разрядностью идентификаторов, указывающих размещение файлов: FAT12, FAT16 и FAT32;
3. exFAT (Extended FAT – расширенная FAT) – развитие файловой системы FAT, использующее 64 разрядные идентификаторы. Применяется в основном для устройств флеш-памяти;
4. CDFS (CD ROM File System) – файловая система для CD дисков, объединяющая форматы ISO 96601 и Joliet2;
5. UDF (Universal Disk Format – универсальный формат дисков) – файловая система для CD и DVD дисков, разработанная для замены ISO 9660.

Основу политики безопасности для компьютерной системы любой организации составляют правила разграничения доступа к объектам компьютерной системы. Разграничение доступа к компьютерным ресурсам базируется на различных моделях управления доступом.

Дискреционная модель разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретного субъекта. Правом редактирования дискреционного списка контроля доступа обычно обладают владелец объекта и администратор безопасности. Эта модель отличается простотой реализации, но возможна утечка конфиденциальной информации даже в результате санкционированных действий пользователей.

В операционных системах Microsoft Windows обычно применяется дискреционное управление доступом к объектам. Объекты разграничения доступа в Windows имеют дескриптор безопасности, содержащий информацию о владельце объекта (его идентификаторе безопасности SID, Security Identifier) и дискреционном списке управления доступом к объекту (Discretionary Access Control List, DACL), правом редактирования которого обладают владелец объекта и администратор. Владелец файла может лишить администратора права изменения разрешений на доступ к объекту. Администратор обладает специальной привилегией смены владельца на другого пользователя, обладающего такой же специальной привилегией (например, на самого себя).

Разграничение доступа к файлам и папкам возможно с помощью Проводника Windows (вкладки Безопасность функций Свойства контекстного меню выделенного объекта).

Права доступа к объектам в операционной системе Windows делятся на специальные, стандартные (общие) и родовые (generic). Специальные права зависят от типа объекта разграничения доступа. Например, к файлам и папкам могут применяться следующие специальные права:

1. обзор папок (выполнение файлов);
2. содержание папки (чтение данных из файла);
3. чтение атрибутов;
4. чтение дополнительных атрибутов;
5. создание файлов (запись данных в файл);
6. создание папок (дозапись данных в файл);
7. запись атрибутов;
8. запись дополнительных атрибутов;
9. удаление подпапок и файлов (только для папок).

Стандартные права доступа к объектам операционной системы Windows не зависят от типа объекта. Определены следующие стандартные права доступа:

1. удаление;
2. чтение разрешений;
3. смена разрешений;
4. смена владельца;
5. синхронизация.

Каждое из родовых разрешений представляет собой логическую группу специальных и стандартных разрешений. Например, для файлов и папок родовое право доступа «Изменение» включает все разрешения кроме «Удаление подпапок и файлов», «Смена разрешений» и «Смена владельца».

Существующие разрешения для пользователя:

1. полный доступ – пользователь, принадлежащий к указанной группе, может выполнять любые операции над папкой;
2. изменить– означает возможность модификации файлов или папки, в зависимости от того, чем является защищаемый объект;
3. чтение и выполнение – возможность чтения и исполнения файлов папки;
4. список содержимого папки – доступ к списку содержимого папки;
5. чтение – доступ на чтение содержимого папки;
6. запись – разрешение на запись означает возможность, изменять или создавать новые файлы, а если такое право доступа стоит для одного файла, то и возможность записи в него группе пользователей или одному пользователю, для которого рядом с этим правом доступа стоит флажок;
7. особые разрешения– используются для уточнения набора прав, которым может обладать пользователь, для их редактирования следует нажать кнопку «Дополнительно», выбрать из списка требуемого пользователя, а потом нажать кнопку «Изменить».

Существующий в Windows механизм наследования облегчает администраторам задачи назначения разрешений и управления ими. Благодаря этому механизму разрешения, установленные для контейнера, автоматически распространяются на все объекты этого контейнера. Например, файлы, создаваемые в папке, наследуют разрешения этой папки.

Если требуется предотвратить наследование разрешений, при настройке особых (отличающихся от родовых) разрешений на доступ к родительской папке (разделу реестра) можно выбрать режим «Применять эти разрешения к объектам и контейнерам только внутри этого контейнера». В случаях, когда необходимо отменить наследование разрешений только для некоторых файлов или подпапок (подразделов реестра), можно отменить режим «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне».

Запрещение права доступа имеет более высокий приоритет, чем его разрешение, если только объект не наследует от различных папок противоречащие друг другу значения этих параметров. В таких случаях в силу вступает значение, унаследованное от родительского контейнера, ближайшего к объекту в иерархической структуре. Дочерние объекты наследуют только наследуемые разрешения.

Для разграничения прав доступа существует несколько способов, наиболее удобными считаются:

1. Вкладка «Безопасность» в свойствах файла или папки.
2. Системная утилита icacls.exe.
3. Файловый менеджер.
4. Средства защиты информации от несанкционированного доступа.
5. Один из простых способов посмотреть какие права получит пользователь к файлу или папке. Для этого в свойствах файла или папки откройте вкладка «Действующие разрешения» окна «Дополнительные параметры безопасности». Для проверки установленных прав следует:
6. перейти во вкладку Действующие разрешения окна Дополнительные параметры безопасности и нажать кнопку «Выбрать»;
7. в появившемся новом окне нажать кнопку «Типы объектов»;
8. из списка выбрать объект (Пользователь, Группа) и нажать кнопку «ОК»;
9. в окне «Выбор»: Пользователь или группа нажать кнопку «Дополнительно»;
10. появится новое окно «Выберите тип объекта»;
11. нажать кнопку «Поиск»;
12. из раскрывшегося списка выбрать пользователя или группу и нажать «ОК»;
13. появится окно с выбранным объектом, нажать кнопку «ОК»;
14. появится список действующих разрешений для выбранного пользователя или выбранной группы.

Постановка задачи. Ознакомиться с теоретическим материалом лабораторной работы и реализовать на практике разграничение прав доступа для заданных папок и файлов, а также настроить политику безопасности, следуя дальнейшим указаниям. Ход работы и результаты зафиксировать в отчете.

Последовательность действий.

Шаг 1. Создать 4-х пользователей (администратор, 2 студента, гость). Созданных пользователей разбить на группы (роли).

Шаг 2. Создать папку (п1) в которой будут папка (п2) с текстовым файлом (ф1) и текстовой файл (ф2). Разграничить права на эти файлы так, чтобы гость не мог зайти и просматривать п1, но мог туда писать. Студенты не могут зайти и писать в п2, но могут читать ее файлы по прямой ссылке (п1/п2/ф1). Так же студенты могут только читать ф2.

Шаг 3. В политике безопасности (локальная политика безопасности) задать следующие пункты:

* 1. Требования сложности пароля.
  2. Максимальный срок действия.
  3. Минимальный срок действия.
  4. Время сброса счетчика блокировки.
  5. Пороговое значение блокировки.
  6. Продолжительность блокировки.

Шаг 4. Результаты оформить в отчет, содержащий цель работы, описание хода выполнения работы, скриншоты с этапами выполнения задания и вывод.

## 1.2. Исследование средств защиты от вредоносного ПО

Цель работы.Целью лабораторной работы является изучение системы защиты от вредоносного программного обеспечения и основ блокировки трафика, а также ознакомление с основными принципами управления архивации.

Поддерживаемые операционные системы.Windows 8.1, Windows 10.

Теоретические сведения. 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 (рис. 1.1.).

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*) (рис 1.2.). Можно не архивировать все подряд, меню «Другие параметры» позволяет выбрать конкретные папки, в которых лежат ваши важные файлы.

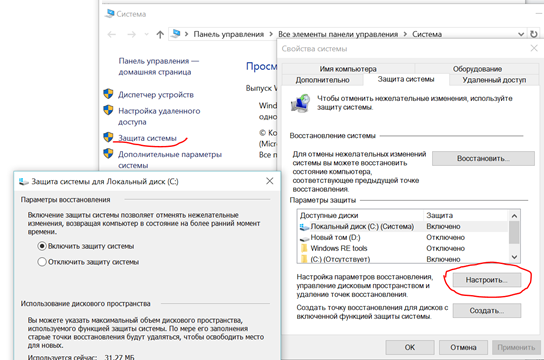


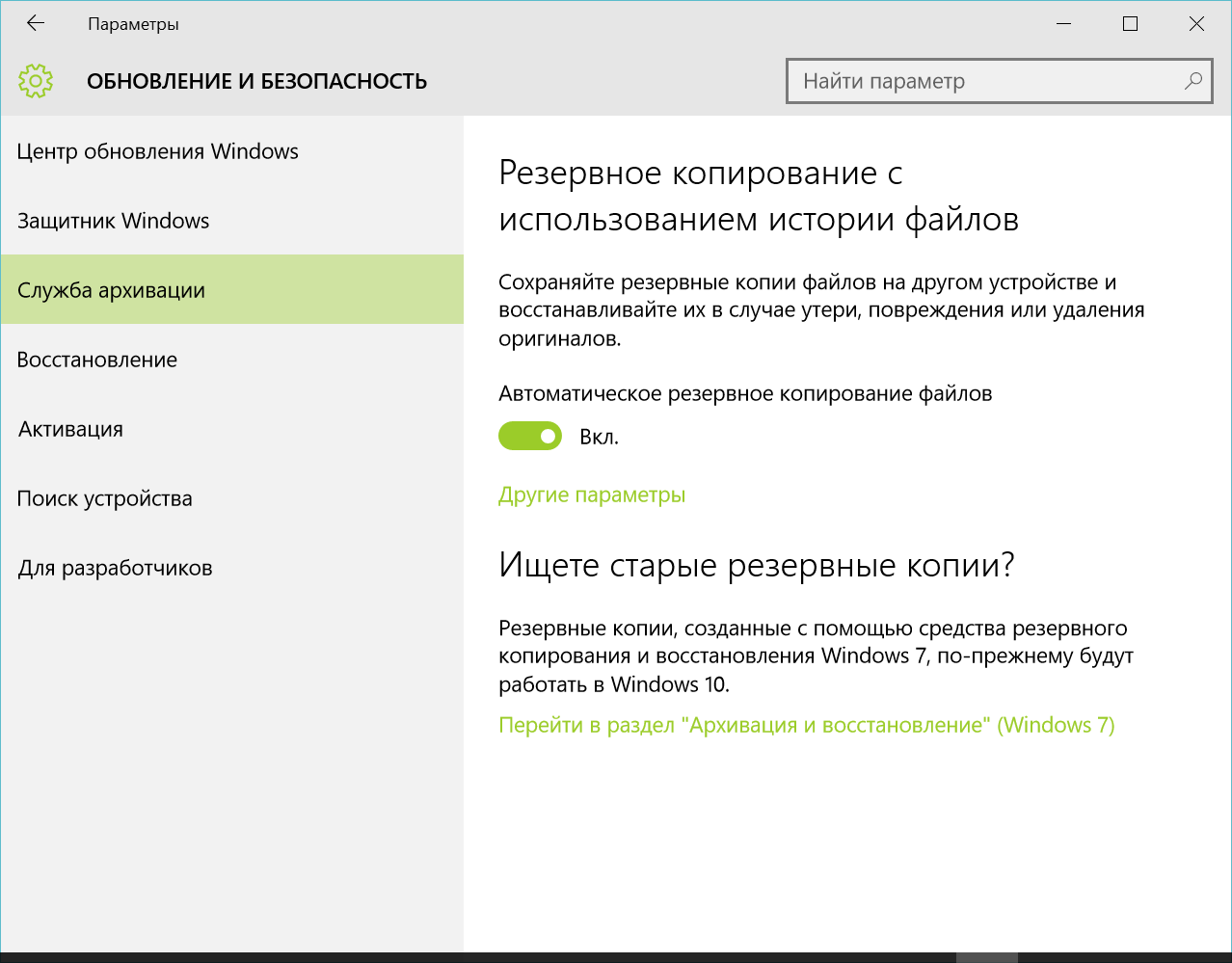
Рис. 1.1. Действия, необходимые для включения защиты системы

Рис. 1.2. Включение резервного копирования файлов

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 включения 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 ОС 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:

1. 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).
2. 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.
3. Назначить правило группе безопасности или отдельному пользователю.
4. Создавать исключения для правил. Например, можно создать правило, разрешающее запуск всех процессов Windows, за исключением редактора реестра (Regedit.exe).
5. Использовать режим "Только аудит" для развертывания политики и выяснения ее влияния перед применением.
6. 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.
7. 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:

1. 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;
2. 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;
3. 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;
4. 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 написать «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 межсетевой экран. Появился в Windows XP SP2. Одним из отличий от предшественника (Internet Connection Firewall) является контроль доступа программ в сеть. Брандмауэр Windows является частью «Центра обеспечения безопасности 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.

Рекомендуется использовать следующие параметры брандмауэра по умолчанию:

1. Брандмауэр включен для всех сетевых подключений.
2. Брандмауэр блокирует все входящие подключения, кроме явно разрешенных пользователем.
3. 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 Брандмауэр Windows.
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:
   1. щелкните или коснитесь «Включить брандмауэр Windows»для каждого типа сети, в котором нужно включить защиту, а затем нажмите ОК;
   2. 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». 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 ему 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.

Постановка задачи. Ознакомиться с теоретическим материалом лабораторной работы и на практике ознакомиться с настройкой архивации истории файлов, а также изучить и настроить SmartScreen, AppLocker и Брандмауэр. Ход работы и результаты зафиксировать в отчете.

Последовательность действий.

Шаг 1. Включить защиту системы Windows. Путь*:* панель управления / система и безопасность / система. Включить защиту системы. Выбрать диск – настройки включить защиту системы.

Шаг 2. Включить отображение расширений.

Шаг 3. Настроить архивацию истории файлов. Создать 2 тестовых файлов. Записать в них одинаковый текст. (Параметры-поиск-история файлов – служба архивации). Далее:

* 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.

Шаг 4. Включить SmartScreen и настроить его на отображение предупреждений: поиск: безопасность и обслуживание.

Шаг 5. Включить AppLocker и запретить пользователям студентам, открывать программу Regedit.exe. А гостю запретить запуск всех программ, кроме Internet Explorer.

Шаг 6. Настроить Брандмауэр (Локальная политика безопасности):

1. Создать исходящее правило. Запретить программу Internet Explorer.
2. Создать входящее правило. Заблокировать порт (любой на ваше усмотрение, продемонстрировать запрет с помощью 2-ой машины).

Шаг 7. Результаты оформить в отчет, содержащий цель работы, описание хода выполнения работы, скриншоты с этапами выполнения задания и вывод.

## 1.3. Исследование средств отражения внешних атак

Цель работы.Целью лабораторной работы является изучение системы защиты конфиденциальных данных и основ аудита, а также ознакомление с основными способами и настройками защиты различных носителей конфиденциальных данных.

Поддерживаемые операционные системы.Windows 8.1, Windows 10.

Теоретические сведения. BitLocker Drive Encryption – [проприетар-ная](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BF%D1%80%D0%B8%D0%B5%D1%82%D0%B0%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) технология, являющаяся частью операционных систем [Microsoft](https://ru.wikipedia.org/wiki/Microsoft) [Windows начиная с версии Vista](https://ru.wikipedia.org/wiki/Windows_Vista) Ultimate.

BitLocker позволяет защищать данные путем полного шифрования диска(ов): логических, карт [SD](https://ru.wikipedia.org/wiki/Secure_Digital) и [USB](https://ru.wikipedia.org/wiki/USB)-флешек. Поддерживаются следующие алгоритмы шифрования:

1. [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) 128.
2. [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) 128 c Elephant diffuser (используется по умолчанию).
3. [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) 256.
4. [AES](https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard) 256 c Elephant diffuser.

Trusted Platform Module (TPM) – название спецификации, описывающей криптопроцессор, в котором хранятся криптографические ключи для защиты информации.

Сам ключ может храниться в [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) или на [USB](https://ru.wikipedia.org/wiki/USB)-устройстве, либо же на компьютере. В случае с [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) при загрузке компьютера ключ может быть получен из него сразу, либо только после аутентификации с помощью USB-ключа или ввода [PIN-кода](https://ru.wikipedia.org/wiki/PIN-%D0%BA%D0%BE%D0%B4) пользователем. Таким образом, возможны следующие комбинации для доступа:

1. [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module).
2. [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) + [PIN](https://ru.wikipedia.org/wiki/PIN-%D0%BA%D0%BE%D0%B4).
3. [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) + [PIN](https://ru.wikipedia.org/wiki/PIN-%D0%BA%D0%BE%D0%B4) + [USB](https://ru.wikipedia.org/wiki/USB)-ключ.
4. [TPM](https://ru.wikipedia.org/wiki/Trusted_Platform_Module) + [USB](https://ru.wikipedia.org/wiki/USB)-ключ.
5. [USB](https://ru.wikipedia.org/wiki/USB)-ключ (данный режим требует активации через групповые политики).
6. Пароль (данный режим доступен начиная с Windows 8, а также требует активации через групповые политики).

BitLocker шифрует том, а не физический диск. Том может занимать часть диска, а может включать в себя массив из нескольких дисков. Для работы BitLocker в случае шифрования системного диска потребуется два NTFS-тома, один для операционной системы и один для загрузочной части. Последний должен быть не менее 1,5 Гб, и не будет зашифрован. Начиная с Windows Vista SP1 появилась возможность шифровать несистемные тома. После создания разделов необходимо инициализировать TPM-модуль в ПК, где он есть, и активировать BitLocker. В Windows 7 появился BitLocker To Go, позволяющий шифровать сменные носители, а также снижены требования для загрузочной части, для нее достаточно 100 Мб.

*Механизмы расшифровки и их уязвимости*

Существует три механизма проверки подлинности, которые можно использовать для реализации BitLocker шифрования:

1. Прозрачный режим работы: этот режим использует возможности аппаратного обеспечения [TPM](https://ru.wikipedia.org/wiki/TPM) для предоставления прозрачной работы пользователей. Пользователи входят на [компьютер](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) с операционной системой Windows, как обычно. Ключ, используемый для шифрования диска, закодирован в чип TPM, и он может быть выдан только в коде [загрузчика ОС](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D1%87%D0%B8%D0%BA_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) (если загрузочные файлы, показываются как не измененные). Этот режим уязвим для нападения при холодной загрузке, так как позволяет выключить компьютер и загрузиться злоумышленнику.
2. Режим проверки подлинности пользователя: этот режим предполагает, что [пользователь](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C) прошел некоторую аутентификацию в предзагрузочной среде в виде предварительного ввода PIN-кода. Этот режим уязвим при использовании [буткит-атак](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D1%82%D0%BA%D0%B8%D1%82).
3. Режим USB-ключа: пользователь должен вставить устройство [USB](https://ru.wikipedia.org/wiki/USB) в компьютер, которое содержит ключ запуска, чтобы иметь возможность загрузки в защищенную операционную систему. Обратите внимание, что для этого режима необходимо, чтобы [BIOS](https://ru.wikipedia.org/wiki/BIOS) на компьютере поддерживал чтение устройств USB в загрузочной среде. Этот режим также уязвим к буткит-нападениям.

В Windows 8.1 и Windows 10 BitLocker позволяет пользователям принимать решение зашифровать только свои данные или весь диск целиком. Также была усилена защита от атаки «грубой силой». При обнаружении данной атаки драйвер BitLocker переводится в защищенный режим. Информация не будет расшифрована, пока пользователь не введет 48-символьный пароль восстановления. Также может быть ведено условие, чтобы расшифровка диска происходила только из доверительной сети.

Для настройки политик шифрования необходимо перейти по следующему пути: **Конфигурация компьютера/Административные шаблоны/Компоненты Windows. Этот параметр политики позволяет выбрать шифрование диска** BitLocker**.**

В открывшемся окне возможна настройка BitLocker под различные носители информации.

Для того чтобы непосредственно зашифровать носитель, то необходимо зайти в Панель управления/Система и Безопасность/Шифрование диска BitLocker.

В Windows имеется система **Аудита,** позволяющая отслеживать и журналировать информацию о том, когда, кем и с помощью какой программы были удалены документы. По умолчанию, Аудит не задействован — слежение само по себе требует определенный процент мощности системы, а если записывать все подряд, то нагрузка станет слишком большой. Тем более, далеко не все действия пользователей могут нас интересовать, поэтому политики Аудита позволяют включить отслеживание только тех событий, что для нас действительно важны. Система Аудита встроена во все операционные системы **Microsoft Windows NT.**

Для включения аудита зайдите с правами администратора в компьютер, предоставляющий доступ к общим документам, и выполните команду **Start/ Run/gpedit.msc.** В разделе «Computer Configuration» раскройте папку **Windows Settings/ Security Settings/Local Policies/ Audit Policy (**рис 1.3.**).**

Дважды щелкните по политике **Audit object access (Аудит доступа к объектам)** и выберите галочку «**Success».** Этот параметр включает механизм слежения за успешным доступом к файлам и реестру. Действительно, ведь нас интересуют только удавшиеся попытки удаления файлов или папок. Включите Аудит только на компьютерах, непосредственно на которых хранятся отслеживаемые объекты.

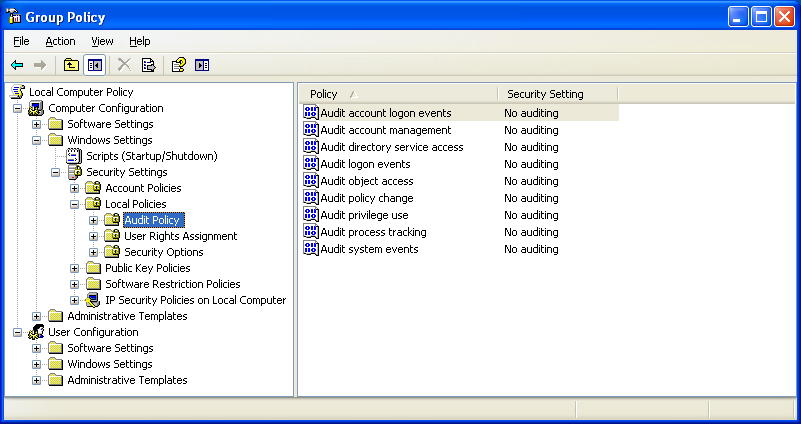
****

Рис. 1.3. Включение аудита

Простого включения политики Аудита недостаточно, мы также должны указать, доступ к каким именно папкам требуется отслеживать. Обычно такими объектами являются папки общих (разделяемых) документов и папки с производственными программами или базами данных, то есть, ресурсы, с которыми работают несколько человек.

Заранее угадать, кто именно удалит файл, невозможно, поэтому слежение и указывается за Всеми (Everyone). Удавшиеся попытки удаления отслеживаемых объектов любым пользователем будут заноситься в журнал. Вызовите свойства требуемой папки (если таких папок несколько, то всех их по очереди) и на закладке **Security (Безопасность)/Advanced (Дополнительно)/Auditing (Аудит)** добавьте слежение за субъектом **Everyone (Все),** его успешными попытками доступа «**Delete» (Удаление)**и**«Delete Subfolders and Files» (Удаление подкаталогов и файлов) (рис 1.4.).**

Событий может журналироваться довольно много, поэтому также следует отрегулировать размер журнала Security (Безопасность), в который они будут записываться.

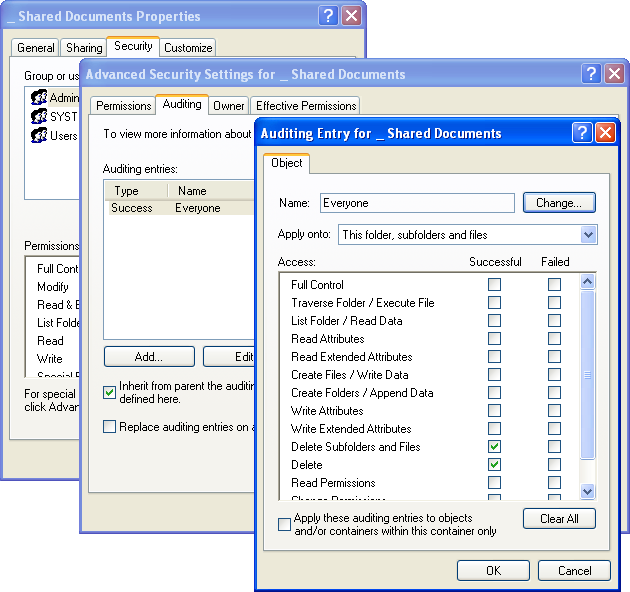


Рис. 1.4. Настройка слежения за объектом

Для этого выполните команду Start /Run/eventvwr.msc. В появившемся окне вызовите свойства журнала Security и укажите следующие параметры:

1. Maximum Log Size = 65536 KB (для рабочих станций) или 262144 KB (для серверов).
2. Overwrite events as needed.

На самом деле, указанные цифры не являются гарантированно точными, а подбираются опытным путем для каждого конкретного случая.

Для проверки журнала нажмите Start/Run/eventvwr.msc и откройте для просмотра журнал «Security» (Безопасность). Журнал может быть заполнен событиями, прямого отношения к проблеме не имеющими. Щелкнув правой кнопкой по журналу «Security», выберите команду View/ Filter и отфильтруйте просмотр по следующим критериям:

1. Event Source: Security;
2. Category: Object Access;
3. Event Types: Success Audit;
4. Event ID: 4663.

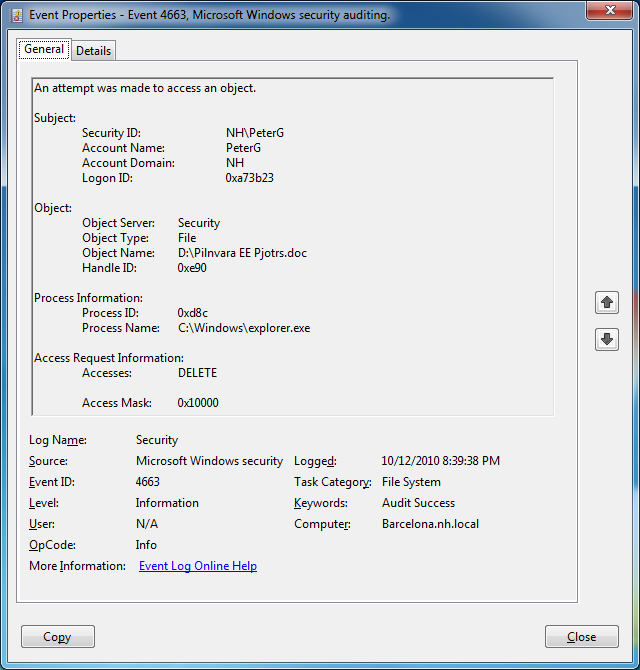


Рис. 1.5. Просмотр свойств события

Не спешите интерпретировать все удаления как злонамеренные. Эта функция зачастую используется при обычной работе программ — например, исполняя команду «**Save» (Сохранить),** программы пакета «**Microsoft Office»** сначала создают новый временный файл, сохраняют в него документ, после чего удаляют предыдущую версию файла. Аналогично, многие приложения баз данных при запуске сначала создают временный файл блокировок **(.lck),** затем удаляют его при выходе из программы.

Постановка задачи. Ознакомиться с теоретическим материалом лабораторной работы и на практике изучить BitLocker и возможности шифрования различных носителей, а также настроить политику аудита в соответствии с предложенным заданием. Ход работы и результаты зафиксировать в отчете.

Последовательность действий.

Шаг 1. Перед выполнением работы сделайте снимок текущего состояния виртуальной машины, чтобы в случае ошибки откатиться на стартовую позицию.

Шаг 2. Необходимо настроить BitLocker в общем плане и отдельно для каждого носителя в соответствии с пунктами ниже:

1. Выбрать метод шифрования AES с 256.
2. Съемные носители:
   1. включить для съемных носителей;
   2. включить использование программного шифрация, а не аппаратное;
   3. шифрование только занятого места;
   4. установить требования сложности пароля для шифрования 8 символов;
   5. включить восстановление съемного носителя.
3. Несъемные носители:
   1. запретить запись данных на незащищенные BitLocker носители;
   2. использовать программное шифрование;
   3. полное шифрование диска;
   4. установить обязательный сложный пароль 8 символов;
   5. включить восстановление диска с помощью 48 битного ключа.
4. Диск операционной системы:
   1. разрешить загрузку и проверка целостности;
   2. установить минимальную длину пин-кода 5 символов;
   3. использовать только программного шифрования;
   4. разрешить пользователю выбирать тип шифрования;
   5. поставить сложный пароль длиной 8 символов;
   6. установить метод восстановления диска. Ключ 48-бит.

Шаг 3. После необходимой настройки переходим к непосредственному шифрованию различных носителей информации.

Рекомендуется сделать еще один снимок виртуальной машины, так как будет необходимо шифровать один и тот же логический том различными способами с различными средствами расшифровки.

При выполнении следующих пунктов необходимо будет проделать и зафиксировать этапы шифрования (выбор необходимых условий) носителей, этапы расшифровки носителей при предоставлении пароля доступа, usb устройства и пароля восстановления:

1. Зашифровать диск с ОС.
   1. Сделать, чтобы при запуске системы(расшифровки) требовался пароль.
      1. сохранить пароль восстановления на флэшке;
      2. сохранить на USB-устройстве флэш памяти.
   2. Сделать, чтобы при запуске системы требовалось USB устройство;
2. Зашифровать второй том.
   1. Сделать, чтобы при расшифровке диска требовался пароль;
   2. Сохранить ключ восстановления в файле.
3. Зашифровать USB флэшку.
   1. Сделать, чтобы при расшифровке носителя требовался пароль;
   2. Сохранить в файл пароль восстановления.

Шаг 4. Необходимо настроить политику аудита, как было показано в пункте в ***«***Теоретических сведениях**»** и в соответствии с заданием ниже.

Для набора файлов и папок, которые создавались в 1-ой лабораторной работе, настроить проверку на удаления. Один из пользователей «студент 1» должен удалить файл ф1. Нужно показать процесс настройка политики аудита. В журнале Аудита продемонстрировать успешный вход «студента 1» и удаление им файла ф1. Так же для пользователя «гость» показать в журнале неудачную попытку доступа к папке п1.

Шаг 5. Результаты оформить в отчет, содержащий цель работы, описание хода выполнения работы, скриншоты с этапами выполнения задания и вывод.

# СРЕДСТВА ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX

## Создание базовой конфигурации

Цель работы.Целью лабораторной работы является изучение типов учетных записей пользователей и основ разграничения доступа пользователей, а также ознакомление с основными принципами управления учетными записями.

Поддерживаемые операционные системы.Debian 8.

Теоретические сведения. Пользователь– это человек, пользующийся ресурсами и возможностями, которые ему предоставляет тот или иной сервис. Пользователь не обязан знать все аспекты функционирования этих сервисов, все, что ему необходимо знать – это как пользоваться ими.

В Linux каждый пользователь имеет свой уникальный числовой идентификатор, по которому он идентифицируется в системе. Этому идентификатору для более удобной работы соответствует имя пользователя. Например, для привилегированного пользователя root зарезервирован нулевой идентификатор.

Все имена пользователей Linux и соответствующие им идентификаторы хранятся в специальном файле passwd. Этот файл располагается в каталоге etc, который, в свою очередь, находится в корневом каталоге системы. Файл имеет обычную текстовую форму.

Пример строки файла: *root:x:0:0:root:/root:/bin/bash.*

Структура строки: *login : password : UID : GID : GECOS : home : shell.*

Каждая запись в файле разделена двоеточиями на 7 частей:

1. Регистрационное имя или логин. Это поле содержит регистрационное имя пользователя. Для операционной системы не важно, какое имя имеет пользователь, система ориентируется на идентификатор, а имя играет, пожалуй, только информационное значение для человека, работающего в системе.
2. Поле пароля. Это поле в ранних версиях Linux содержало зашифрованный пароль, а теперь, когда была введена технология теневых паролей, в этом поле просто ставится *x.* Практического применения это поле не имеет.
3. Идентификатор пользователя (UID). В системе Linux каждый пользователь имеет уникальный идентификационный номер, который однозначно определяет его в системе.
4. Идентификатор группы, к которой принадлежит этот пользователь (GID).
5. Информационное поле GECOS. Поле GECOS хранит вспомогательную информацию о пользователе (номер телефона, адрес, полное имя и так далее). Оно не имеет четко определенного синтаксиса.
6. Полный путь к домашнему каталогу пользователя. В ОС Linux для каждого пользователя создается его домашний каталог, в котором он может хранить свои документы. Обычно эти каталоги располагаются в директории /home корневого каталога и по умолчанию имеют имена владельцев.
7. Путь к командной оболочке. Последнее поле содержит полный путь к рабочей оболочке пользователя (по умолчанию такой оболочкой является bash). Эта оболочка запускается, когда пользователь проходит процедуру аутентификации.

Этот файл, как правило, не редактируется вручную, хотя это вполне допустимо. Обычно для редактирования файла пользователей используют специальные команды: useradd, usermod и userdel.

1. Useradd – Позволяет добавить нового пользователя в систему.

2. Usermod – Позволяет изменять такие параметры, домашний каталог, группа, идентификатор пользователя и так далее.

1. Userdel – Позволяет удалить пользователя.

Каждый пользователь в системе имеет свой собственный пароль. Наличие пароля – необходимая составляющая политики безопасности пользователей Linux. Пароли хранятся в отдельном файле /etc/shadow.

Пример строки файла /etc/shadow:

*root:$1$gka0eOIt$3RXPSZVX9AMLVZ65gXmQA1:13766:0:::::*

Файл shadow, по аналогии с файлом passwd, разделен на несколько частей двоеточиями (поля 3 – 8 являются необязательными) :

1. Имя пользователя. Это поле просто дублируется из файла passwd.
2. Хэш пароля. Пароль в Linux никогда не хранится в открытом виде.
3. Содержит число дней, прошедших с полуночи 01.01.1970 до дня последнего изменения пароля.
4. Содержит минимальное число дней действия пароля со дня его последнего изменения.
5. Содержит максимальное число дней действия пароля.
6. Содержит число дней до даты, когда система начнет выдавать предупреждения о необходимости смены пароля.
7. Содержит число дней со времени обязательной смены пароля до блокировки учетной записи.
8. Содержит день блокировки учетной записи.

Файл паролей имеет права только на чтение и только для суперпользователя (права доступа будут описаны ниже). Его содержимое является недоступным для рядовых пользователей, таким образом, исключается возможность раскрытия зашифрованного пароля.

Изменения пароля в Linux происходит с использованием специальной программы passwd. В качестве параметра в командной строке она получает имя пользователя и при запуске требует ввода пароля для этого пользователя.

Для более удобного управления доступом к ресурсам в Linux все пользователи объединяются в группы. В данном случае группа– это множество пользователей, объединенных по каким-либо критериям.

Пример строки файла /etc/group: *bin:x:1:root,bin,daemon.*

Каждая запись файла /etc/group разделена двоеточиями на 4 части:

1. Символьное имя группы.
2. Пароль группы – устаревшее поле, не используется.
3. Уникальный идентификатор группы, или GID.
4. Список имен участников, разделенных запятыми.

Всем файлам, созданным пользователем после регистрации в системе, будет автоматически присвоен этот номер группы.

*Права пользователя.*

Концепция файловой политики безопасности Linux строится на том, что любой файл системы имеет 3 категории владельцев: собственно, владельца файла или, проще говоря, его создателя, какую-либо группу пользователей, в которую чаще всего входит владелец файла, и всех остальных. Таким образом, привилегированный пользователь или владелец файла, поскольку только он имеет возможность изменять права доступа, может построить политику файловой безопасности, определяя права отдельно для владельца файла, для группы пользователей и для всех остальных пользователей системы.

Права доступа к файлу или каталогу описываются тремя восьмеричными цифрами, самая левая из которых – права доступа владельца, средняя – права группы, правая – права доступа для всех остальных. Каждая из этих восьмеричных цифр представляет собой битовую маску из 3-х бит. Эти биты отвечают за право на чтение, запись и исполнение файла или каталога. Если бит установлен в 1 – операция разрешена, если в 0 – запрещена.

*Таблица*

|  |  |  |  |
| --- | --- | --- | --- |
| Восьмеричное  описание | Символьное  описание | Права доступа | |
| на файл | на директорию |
| 0 | --- | нет | нет |
| 1 | --x | выполнение | чтение файлов и их свойств |
| 2 | -w- | запись | нет |
| 3 | -wx | запись и выполнение | все, кроме чтения списка файлов |
| 4 | r-- | чтение | чтение имен файлов |
| 5 | r-x | чтение и выполнение | доступ на чтение |
| 6 | rw- | чтение и запись | чтение имен файлов |
| 7 | rwx | все права | все права |

Какие права доступа определены для каждого файла, можно узнать, просмотрев атрибуты файла, набрав в терминале команду ls с ключом –l (рис. 2.1.):

1. Права доступа (владельца, группы, остальных).
2. Количество жестких ссылок.
3. Владелец файла.
4. Группа владельца файла.
5. Размер файла, в байтах.
6. Дата последний модификации файла.
7. Имя файла.



Рис. 2.1. Права доступа для файла

Биты доступа (рис 2.2.):

1. Тип файла [- (file), d (dir), l (link), c (char dev), b (block dev), s (socket), p (FIFO)].
2. Права пользователя – владельца файла.
3. Права группы – владельца файла.
4. Права остальных пользователей.

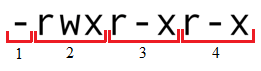


Рис. 2.2. Биты доступа

Изменение прав доступа к файлу осуществляется при помощи стандартной системной команды chmod. Права доступа при вызове команды могут задаваться как битовой маской в десятичном представлении, так и при помощи символов (рис 2.3.):

1. u – user;
2. g – group;
3. – other;
4. a – all;
5. + –добавить;
6. - – убрать;
7. = – установить.



Рис. 2.3. Команда chmod

Установка битов доступа (рис 2.4.):

1. 1 — бит доступа установлен;
2. 0 — бит доступа не установлен.



Рис. 2.4. Установка битов доступа

Пример: # chmod 754 somefile.

Основные команды необходимые для выполнения работы: addgroup, adduser, chmod, chown, passwd.

Постановка задачи. Ознакомиться с теоретическим материалом лабораторной работы и на практике изучить настройку разграничения прав доступа пользователей, а также настроить политику безопасности в соответствии с предложенным заданием. Ход работы и результаты зафиксировать в отчете.

Последовательность действий.

Шаг 1. Создать две группы students, teachers. Создать 4-х пользователей (администратор (root- создается при установке системы), teacher, student1, student2). Пользователей студент1 и студент2 объединить в группу. Пользователей администратор и преподаватель объединить в группу.

Шаг 2. Создать папку (dir1) c текстовыми файлами file1 и file2. Создать папку (dir2) с текстовыми файлами file3 и file4.

Разграничить права доступа на эти файлы так:

1. /dir1/file1 – Доступ студентам только на чтение, остальным все разрешено.
2. /dir1/file2 – Полные права student1, остальным все запрещено.
3. /dir2 – Полный доступ группе преподавателей. Студентам запрещено просматривать содержание директории и писать в нее.
4. /dir2/file3 – Полный доступ группе преподавателей. Студентам доступ по прямой ссылке /dir2/file3.
5. /dir2/file4 – Доступ только группе преподавателей.

Шаг 3. В политике безопасности (с помощью команды passwd) задать следующие пункты:

1. Максимальный срок действия – 30 дней.
2. Минимальный срок действия – 10 дней.
3. Предупреждение о скорой смене пароля – 5 дней.
4. Срок блокировки учетной записи с момента истечения пароля 15 дней.

Шаг 4. Результаты оформить в отчет, содержащий цель работы, описание хода выполнения работы, скриншоты с этапами выполнения задания и вывод.

## Изучение подсистемы безопасности в ОС Linux

Цель работы.Целью лабораторной работы является изучение модификаторов доступа SUID, SGUID, а также ознакомление с расширенными настройками прав доступа к файлам и каталогам и утилитой для управления работой межсетевым экраном iptables.

Поддерживаемые операционные системы.Debian 8.

Теоретические сведения. В Unix-подобных системах приложение запускается с правами пользователя, вызвавшего указанное приложение. Это обеспечивает дополнительную безопасность, так как процесс с правами пользователя не сможет получить доступ на запись к важным системным файлам, например /etc/passwd, который принадлежит суперпользователю root. Если на исполняемый файл установлен бит SUID, то при выполнении эта программа автоматически меняет «эффективный userID» на идентификатор того пользователя, который является владельцем этого файла. То есть, независимо от того *–* кто запускает эту программу, она при выполнении имеет права хозяина этого файла.

Аналогичная ситуация с GUID *–* запуск будет выполнен с правами группы, которой принадлежит файл:

1. Восьмеричные значения для SUID и SGID – 4000и 2000.
2. Символьные: u+s и g+s.

Установить SUID и SGID можно командой chmod:

1. chmod u+s file1.sh – устанавливает на файл file1.sh бит SUID;
2. chmod g+s file1.sh – устанавливает на файл file1.sh бит GUID.

Проверить установку модификатора доступа можно просмотрев права доступа: -rwxrwsrwx 1 root root 0 2016-04-08 16:16 file1.

Видно, что для файла установлен SGID, о чем свидетельствует символ «**s**» (-rwxrwsrwx).

Еще одно важное усовершенствование касается использования sticky-бита в каталогах. Каталог с установленным sticky-битом означает, что удалить файл из этого каталога может только владелец файла или суперпользователь. Другие пользователи лишаются права удалять файлы. Установить sticky-бит в каталоге может только суперпользователь. Sticky-бит каталога, в отличие от sticky-бита файла, остается в каталоге до тех пор, пока владелец каталога или суперпользователь не удалит каталог явно или не применит к нему chmod. Заметьте, что владелец может удалить sticky-бит, но не может его установить.

1. Восьмеричное значение sticky-бита: 1000.
2. Символьное: +t.

Установить sticky-бит на каталог можно используя команду chmod:

1. chmod 1755 dir **–** с заменой прав;
2. chmod +t dir **–** добавление к текущим правам.

Проверить установку модификатора доступа можно просмотрев права доступа: drwxr-xr-t 2 root root 4096 2016-04-08 16:18 student.

Видно, что для файла установлен Sticky-бит, о чем свидетельствует символ «**t**» (drwxr-xr-t).

*Access Control List – списки контроля доступа*

Для реализации сложных структур прав доступа используются расширенные права – ACL (Access control list – cписки контроля доступа).

Списки контроля доступом (ACL) дают большую гибкость, чем стандартный набор полномочий «пользователь/группа/остальные».

Существуют два типа ACL:

1. ACL для доступа– это список управления доступом для заданного файла или каталога. Проще говоря – это сами права на объект, которые будут контролировать доступ к этому объекту.
2. ACL по умолчанию – может быть связан только с каталогом, и, если файл в этом каталоге не имеет ACL для доступа, используются правила, определенные в ACL по умолчанию. ACL по умолчанию являются необязательными.

Управления ACL списками осуществляется всего лишь двумя командами: setfacl, getfacl.

Утилита getfacl: Выводит листинг ACL прав для указанных объектов.

Примеры использования:

1. getfacl \* – отобразит права ACL для всех объектов в текущем каталоге;
2. getfacl file.txt – отобразить ACL для файла file.txt;
3. getfacl -R \* – отобразит ACL для всех объектов (включая подкаталоги и их содержимое) текущего каталога.

Чтобы посмотреть, установлены ли ACL на объектах, достаточно воспользоваться командой ls -l: -rwxr-x---+ 1 root root 19 2016-04-08 16:20 file.

Видно, что для файла установлен ACL, о чем свидетельствует символ «**+**» (-rwxr-x—+).

Пример вывода команды getfacl для file:

1. # file: qwert – Имя файла;
2. # owner: root – Владелец файла (основные права Unix);
3. # group: root – Группа файла (основные права Unix);
4. user::rwx – Права для владельца файла (основные права Unix);
5. user:child:rw- – Права ACL для пользователя child;
6. group::r-- – Права для группы файла (основные права Unix);
7. mask::rw- – Эффективная маска;
8. other::--- – Права для пользователя "все остальные".

Утилита setfacl: предназначена для установки, модификации или удаления ACL.

Списки ACL можно задать:

1. На уровне пользователей *–* назначаются ACL конкретным пользователям.
2. На уровне групп *–* назначаются ACL конкретным группам.
3. С помощью маски эффективных прав – ограничение максимальных прав для пользователей и/или групп.
4. Для пользователей, не включенных в группу данного файла *–* это т.н. пользователь «Все остальные».

Рассмотрим простой синтаксис setfacl: setfacl <опции> <ключ> <список правил> <объект>.

1. <опции> *–* задает дополнительные опции;
2. <ключ> *–* задает режим работы утилиты;
3. <список правил> – собственно, сами правила доступа к объекту;
4. <объект> *–* объект к которому применяется ACL, в большинстве случаев это файл или каталог.

Часто используемые ключи:

1. --set или --set file\* *–* Устанавливает новые указанные права ACL, удаляя все существующие. Необходимо, чтобы наравне с задаваемыми правилами ACL были также указаны стандартные права Unix, в противном случае будет давать ошибку;
2. -m или -M file\* *–* Модифицирует указанные ACL на объекте. Другие существующие ACL сохраняются.
3. -x или -X file\* *–* Удаляет указанные ACL права с объекта. Стандартные права Unix не изменяются.

Часто используемые опции:

1. -b *–* Удаляет все ACL права с объекта, сохраняя основные права;
2. -k *–* Удаляет с объекта ACL по умолчанию. Если таковых на объекте нет, предупреждение об этом выдаваться не будет;
3. -d *–* Устанавливает ACL по умолчанию на объект;
4. -R *–* Рекурсивное назначение (удаление) прав.

Формирование списка правил:

1. u:<uid>:<perms>\* *–* Назначает ACL для доступа заданному пользователю. Здесь можно указать имя или UID пользователя. Это может быть любой пользователь, допустимый в данной системе.
2. g:<gid>:<perms>\* *–* Назначает ACL для доступа заданной группе. Здесь можно указать имя или GID группы. Это может быть любая группа, допустимая в данной системе.
3. o:<perms>\* *–* Назначает ACL для доступа пользователям, не включенным в группу файла. Это пользователь «все остальные», как в стандартных правах Unix.

Пример установки прав: setfacl -m u:student:rw file.txt.

Назначает пользователю student права на чтение и запись file.txt.

Дополнительную информацию по утилитам getfacl и setfacl смотрите в соответствующих man руководствах.

*IPTables*

IPTables утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) netfilter.

Ключевыми понятиями в IPTables являются:

1. Правило *–* состоит из критерия, действия и счетчика. Если пакет соответствует критерию, к нему применяется действие, и он учитывается счетчиком. Критерия может и не быть — тогда неявно предполагается критерий «все пакеты». Указывать действие тоже не обязательно — в отсутствие действия правило будет работать только как счетчик.
2. Критерий *–* логическое выражение, анализирующее свойства пакета и/или соединения и определяющее, подпадает ли данный конкретный пакет под действие текущего правила.
3. Действие *–* описание действия, которое нужно проделать с пакетом и/или соединением в том случае, если они подпадают под действие этого правила. О действиях более подробно будет рассказано ниже.
4. Счетчик *–* компонент правила, обеспечивающий учет количества пакетов, которые попали под критерий данного правила. Также счетчик учитывает суммарный объем таких пакетов в байтах.
5. Цепочка *–* упорядоченная последовательность правил. Цепочки можно разделить на пользовательские и базовые:
6. Базовая цепочка *–* цепочка, создаваемая по умолчанию при инициализации таблицы. Каждый пакет, в зависимости от того, предназначен ли он самому хосту, сгенерирован им или является транзитным, должен пройти положенный ему набор базовых цепочек различных таблиц. Схема следования пакетов приведена на рисунке. Кроме того, базовая цепочка отличается от пользовательской наличием «действия по умолчанию» (default policy). Это действие применяется к тем пакетам, которые не были обработаны другими правилами этой цепочки и вызванных из нее цепочек (см. переходы). Имена базовых цепочек всегда записываются в верхнем регистре (PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING);
7. Пользовательская цепочка*–* цепочка, созданная пользователем. Может использоваться только в пределах своей таблицы. Рекомендуется не использовать для таких цепочек имена в верхнем регистре, чтобы избежать путаницы с базовыми цепочками и встроенными действиями.
8. Таблица*–* совокупность базовых и пользовательскихцепочек, объединенных общим функциональным назначением. Имена таблиц (как и модулей критериев) записываются в нижнем регистре, так как в принципе не могут конфликтовать с именами пользовательских цепочек. При вызове команды iptables таблица указывается в формате -t имя\_таблицы. При отсутствии явного указания, используется таблица filter. Более подробно таблицы будут рассмотрены ниже.

*Таблицы IPTABLES*

У IPTABLES имеется 4 встроенных типа таблиц:

1. Filter Table

Является таблицей по умолчанию. Если при создании/изменении правила не указана таблица – используется именно filter. Используется в основном для фильтрации пакетов. К примеру, тут можно выполнить DROP, LOG, ACCEPT или REJECT без каких-либо сложностей, как в других таблицах. Использует 3 встроенных цепочки:

1. INPUT chain – входящие пакеты, используется только для пакетов, цель которых – сам сервер, не используется для транзитного (роутинга) трафика;
2. OUTPUT chain – исходящие пакеты, созданные локально и отправленные “за пределы” сервера;
3. FORWARD chain – пакеты, предназначенные другому сетевому интерфейсу (роут на другие машины сети, например).
4. NAT table

Таблица nat используется главным образом для преобразования сетевых

адресов (Network Address Translation). Через эту таблицу проходит только первый пакет из потока. Преобразования адресов автоматически применяется ко всем последующим пакетам. Это один из факторов, исходя из которых мы не должны осуществлять какую-либо фильтрацию в этой таблице.

1. PREROUTING chain – преобразование адресов DNAT (Destination Network Address Translation), фильтрация пакетов здесь допускается только в исключительных случаях;
2. POSTROUTING chain – выполняется преобразование адресов SNAT (Source Network Address Translation), фильтрация пакетов здесь крайне нежелательна;
3. OUTPUT chain – NAT для локально сгенерированных пакетов.
4. Mangle table

Таблица Mangle предназначена только для внесения изменения в некоторые заголовки пакетов – TOS (Type of Service), TTL (Time to Live), MARK (особая метка для IPTABLES или других служб). Важно: в действительности поле MARK не изменяется, но в памяти ядра заводится структура, которая сопровождает данный пакет все время его прохождения через машину, так что другие правила и приложения на данной машине (и только на данной машине) могут использовать это поле в своих целях.

Включает в себя такие цепочки:

1. PREROUTING chain;
2. OUTPUT chain;
3. FORWARD chain;
4. INPUT chain;
5. POSTROUTING chain.
6. Raw table

Применяется до передачи пакета механизму определения состояний (state machine, connection tracking – система трассировки соединений, при помощи которой реализуется межсетевой экран на сеансовом уровне (stateful firewall), позволяет определить, к какому соединению или сеансу принадлежит пакет, анализирует все пакеты кроме тех, которые были помечены NOTRACK в таблице raw).

1. PREROUTING chain;
2. OUTPUT chain.

*Цепочки IPTABLES*

Существует 5 типов стандартных цепочек, встроенных в систему:

PREROUTING *–* для изначальной обработки входящих пакетов;

INPUT *–* для входящих пакетов, адресованных непосредственно локальному процессу (клиенту или серверу);

FORWARD *–* для входящих пакетов, перенаправленных на выход (заметьте, что перенаправляемые пакеты проходят сначала цепь PREROUTING, затем FORWARD и POSTROUTING);

OUTPUT *–* для пакетов, генерируемых локальными процессами;

POSTROUTING *–* для окончательной обработки исходящих пакетов.

Схематично путь пакетов через IPTABLESхорошо представлен на следующей схеме (рис. 2.5):



Рис. 2.5. Путь пакетов по цепочкам IPTABLES

*Правила IPTABLES*

Правила имеют следующую структуру: правило > цель > счетчик.

Если пакет соответствует правилу, к нему применяется цель, и он учитывается счетчиком. Если правило (или критерий) не задан – то цель применяется ко всем проходящим через цепочку пакетам. Если не указаны ни цель, ни правило – для правила будет срабатывать только счетчик пакетов. Если пакет не попадает под правило и цель – он передается следующему правилу в списке.

Цели (targets) IPTABLES

Правило может содержать одно из следующих целей (наиболее часто встречаемые, полный список в соответствующем man руководстве):

1. ACCEPT – принять пакет, и передать следующей цепочке (или приложению, или передать для дальнейшего роутинга);
2. DNAT – (Destination Network Address Translation) используется для преобразования адреса места назначения в IPзаголовке пакета. Если пакет подпадает под критерий правила, выполняющего DNAT, то этот пакет, и все последующие пакеты из этого же потока, будут подвергнуты преобразованию адреса назначения и переданы на требуемое устройство, хост или сеть. Действие DNAT может выполняться только в цепочках PREROUTING и OUTPUT таблицы nat, и во вложенных под-цепочках. Важно запомнить, что вложенные подцепочки, реализующие DNAT не должны вызываться из других цепочек, кроме PREROUTING и OUTPUT;
3. DROP – просто “сбрасывает” пакет и IPTABLES“забывает” о его существовании. “Сброшенные” пакеты прекращают свое движение полностью, т.е. они не передаются в другие таблицы, как это происходит в случае с действием ACCEPT. Следует помнить, что данное действие может иметь негативные последствия, поскольку может оставлять незакрытые “мертвые” сокеты как на стороне сервера, так и на стороне клиента, наилучшим способом защиты будет использование действия REJECT, особенно при защите от сканирования портов;
4. REDIRECT – выполняет перенаправление пакетов и потоков на другой порт той же самой машины. Пакеты, поступающие на HTTP порт можно перенаправить на порт HTTP-proxy. Удобен для выполнения “прозрачного” проксирования (transparent proxy), когда машины в локальной сети даже не подозревают о существовании прокси. Может использоваться только в цепочках PREROUTING и OUTPUT таблицы nat;
5. REJECT – используется, как правило, в тех же самых ситуациях, что и DROP, но в отличие от DROP, команда REJECT выдает сообщение об ошибке на хост, передавший пакет;
6. RETURN – прекращает движение пакета по текущей цепочке правил и производит возврат следующему правилу в вызывающей (предыдущей) цепочке, если текущая цепочка была вложенной, или, если текущая цепочка лежит на самом верхнем уровне (например, INPUT), то к пакету будет применена «политика по умолчанию». Обычно, в качестве «политики по умолчанию» назначают действия ACCEPT или DROP.

Критерий так же может использовать состояние пакета для принятия решений:

1. NEW – пакет открывает новый сеанс, например – пакет TCP с флагом SYN;
2. ESTABLISHED – пакет является частью уже существующего сеанса;
3. RELATED – пакет открывает новый сеанс, связанный с уже открытым сеансом, например, во время сеанса пассивного FTP, клиент подсоединяется к порту 21 сервера, сервер сообщает клиенту номер второго, случайно выбранного порта, после чего клиент подсоединяется ко второму порту для передачи файлов; в этом случае второй сеанс (передача файлов по второму порту) связан с уже существующим сеансом (изначальное подсоединение к порту 21);
4. INVALID – все прочие пакеты.

Управление IPTables осуществляется с помощью команды iptables. Все ключи можно узнать, прочитав man руководство.

Постановка задачи. Ознакомиться с теоретическим материалом лабораторной работы. На практике изучить модификаторы доступа и расширенные настройки разграничения прав доступа пользователей, а также Произвести настройку межсетевого экрана с использованием iptables. Ход работы и результаты зафиксировать в отчете.

Последовательность действий.

Шаг 1. Описать положительные и отрицательные стороны установки модификаторов SUID, SGUID и Sticky-bit.

Шаг 2. Установить на файл права с использованием ACL, затем задать более жесткие (ограничивающие) базовые правила (при помощи chmod) для пользователя. Посмотреть, что произойдет, какие права будут работать, сделать вывод.

Шаг 3. Создать каталог, установить владельца пользователя teacher. Установить права для teacher – rwx, остальным запретить все. Задать для каталога ACL по умолчанию. В каталоге создать файл и подкаталог, проверить их права. Сделать вывод.

4. Произвести настройку межсетевого экрана с использованием iptables:

1. запретить все соединения (изначально все что не разрешено – запрещено);
2. разрешить локальный траффик;
3. разрешить все уже инициированные входящие соединения, а также их дочерние;
4. разрешить все новые, уже инициированные исходящие соединения, а также их дочерние;
5. открыть порт для SSH (порт 22);
6. открыть порт для HTTP (порт 80);
7. открыть порт для HTTPS (порт 443);
8. разрешить POP3(порт 110) только с IP 173.194.71.17;
9. разрешить DNS (порт 53).

Шаг 5. Результаты оформить в отчет, содержащий цель работы, описание хода выполнения работы, скриншоты с этапами выполнения задания и вывод.

# Список рекомендуемой литературы

Баранчиков А.И., Баранчиков П.А., Пылькин А.Н. Алгоритмы и модели ограничения доступа к записям баз данных: учеб. пособие. М.: Горячая линия-Телеком, 2011.

Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем: учеб. пособие. М.: Изд-во Машиностроение-1, 2007. // Информационная система "Единое окно доступа к образовательным ресурсам": сайт. URL: http://window.edu.ru/resource/669/56669 (дата обращения 17.05.2017).

Брагг Роберта. Система безопасности Windows 2000. М.: Вильямс, 2001. 591 с.

Бэндл Дэвид. Защита и безопасность в сетях Linux. СПб.: Питер, 2002.

Ворона В.А., Тихонов В.А. Комплексные (интегрированные) системы обеспечения безопасности. Учеб. пособие. М.: Горячая линия-Телеком, 2013.

Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие. М.: Горячая линия-Телеком, 2016.

Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий: учеб. пособие. СПб: Изд-во БХВ-Петербург, 2003. 368 с.

Зима В.М., Молдовян А.А., Молдовян Н.А. Защита компьютерных ресурсов от несанкционированных действий пользователей: учеб. пособие. СПб.: типография Военной Академии Связи, 1997.

Зима В.М., Молдовян А.А. Многоуровневая защита информационно-программного обеспечения вычислительных систем: учеб. пособие. СПб.: издательско-полиграфический центр ГЭТУ, 1997.

Зима В.М., Молдовян А.А., Молдовян Н.А. Основы резервирования информации и архивация файловых данных в вычислительных системах: учеб. пособие. СПб.: издательство СПбГУ,1998.

Макаренко С.И. Информационная безопасность: учеб. пособие. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009 // Информационная система "Единое окно доступа к образовательным ресурсам": сайт. URL: http://window.edu.ru/resource/775/77775 (дата обращения 17.05.2017).

Мафтик С. Механизмы защиты в сетях ЭВМ: пер. с англ. М.: Мир. 1993.

Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи: учеб. пособие. СПб.: Изд-во БХВ-Петербург, 2010.

Проскурин В.Г. Защита в операционных системах: учеб. пособие. М.: Горячая линия-Телеком, 2016.

Скембрей Джоел. Секреты хакеров. Безопасность сетей – готовые решения. М.: Вильямс, 2001. 651 с.

Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности: учеб. пособие. М.: Изд-во Молгачева, 2001. 351 с.

Лабораторный практикум

Молдовян Александр Андреевич

Березин Андрей Николаевич

Ковалева Ирина Владиславовна

**Защита операционных систем и систем управления**

**базами данных**

Издание публикуется в авторской редакции

СПбГЭТУ «ЛЭТИ»

197376, Санкт*-*Петербург, ул. Проф. Попова, 5