УНИВЕРСИТЕТ ИТМО

Т.А. Маркина

ОСНОВНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ В ОС MS WINDOWS. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Санкт-Петербург
2020

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

Т.А. Маркина

ОСНОВНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ В ОС MS WINDOWS. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки 09.03.01, 09.03.04
в качестве учебно-методического пособия для реализации основных профессиональных образовательных программ высшего образования бакалавриата,

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург
2020

Маркина Т.А., Основные механизмы защиты в ОС MS Windows. Методические рекомендации по выполнению лабораторных работ – СПб: Университет ИТМО, 2020. – 34 с.

Рецензент(ы):
Балакшин Павел Валерьевич, кандидат технических наук, доцент факультета программной инженерии и компьютерной техники, Университета ИТМО.

Предлагаемое пособие предназначено для академического бакалавриата. В пособии представлены материалы для выполнения и защиты лабораторных работ, а также вопросы для самостоятельной подготовки. Учебно-методическое пособие предназначено для студентов по направлениям подготовки 09.03.04, 09.03.01 в качестве учебного пособия для выполнения лабораторных работ по курсу «Информационная безопасность».

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Содержание

Введение

В предлагаемом пособии представлен цикл лабораторных работ, выполняемых в рамках курса «Информационная безопасность» для основных профессиональных образовательных программ высшего образования бакалавриата по направлениям подготовки 09.03.04, 09.03.01.

Курс посвящен вопросам настройки операционных систем (ОС) Windows для их безопасной работы и взаимодействия, а также основным механизмам защиты как новейших версий ОС семейства Windows, так и ОС предыдущего поколения, которые у большей части организаций эксплуатируются одновременно. Особое внимание уделено практическим работам, иллюстрирующим возможности систем безопасности операционных систем MS Windows.

Описание каждой лабораторной работы содержит теоретический материал, задание на работу и контрольные вопросы. Студенты выполняют задание самостоятельно или в группах. Полученные при этом результаты оформляются в отчеты и защищаются в течение семестра, но не позднее зачетной недели. В лабораторных работах предусматривается текущий контроль, проводимый в форме проверки отчета преподавателем и ответов на его вопросы. Промежуточный контроль проводится в устной форме. В конце пособия приводится список рекомендуемых источников литературы.

Общие методические рекомендации для выполнения представленных в пособии лабораторных работ:

1. Выбрать операционную систему, на которой будут проводиться исследования и выполняться задания.

2. Описать программные и аппаратные средства, используемые при выполнении задания.

3. Выполнить настройки ОС в соответствии с заданиями.

5. Описать содержательно, каким образом была выполнена настройка.

Выполнение лабораторных работ направлено на закрепление теоретических знаний и получение практических навыков при изучении данной дисциплины. В результате освоения материалов пособия обучающийся приобретает следующие умения и навыки:

- Установка специальных средств управления безопасностью сетевых устройств администрируемой сети.

- Установка средств обеспечения безопасности удаленного доступа.
- Настройка средств обеспечения безопасности удаленного доступа.
- Использование современных стандартов при настройке параметров администрируемых устройств и программного обеспечения.
- Использование нормативно-технической документацией в области инфокоммуникационных технологий.

Распределение трудозатрат студентов в аудитории и в процессе СРС представлено в соответствии с программой изучаемой дисциплины. В рамках самостоятельной работы студентам рекомендуется отвести на изучение теоретических материалов по плану лекций каждого раздела ориентировочно по 8 часов, на подготовку и выполнение лабораторных работ и подготовку к промежуточному контролю также ориентировочно по 4 часа, и по 5 часов на самостоятельное изучение дополнительных источников информации.

Данное учебное пособие является переизданием пособия «Основные механизмы защиты в ОС MS Windows. Методические рекомендации по выполнению лабораторных работ», изданного в 2015 году. Были обновлены задания, исправлены ошибки и опечатки.

Правила проведение лабораторных работ

1. В помещение НЕ ДОПУСКАЕТСЯ присутствие студентов:
   - в верхней уличной одежде (при наличии работающего гардероба);
   - с едой, напитками и т.п.
2. Во время проведения лабораторных занятий сотовые телефоны ДОЛЖНЫ быть настроены на беззвучный режим или выключены.
3. Лабораторные работы выполняются группами по 1÷3 человека.
4. Лабораторные работы выполняются исходя из номера варианта, который необходимо получить у преподавателя.
5. Основная часть предусмотрена на оценку «хорошо», для получения оценки «отлично» необходимо выполнить полностью дополнительную часть.

Требования к отчетности

1. Содержание отчета:
   - цель работы;
   - программные и аппаратные средства (процессор, видеокарта, объем оперативной памяти), используемые при выполнении работы;
   - основная часть: описание всех вопросов основной части обязательно отобразить в отчете в строгом порядке;
   - дополнительная часть: описание всех вопросов дополнительной части обязательно отобразить в отчете в строгом порядке;
   - заключение (выводы).
2. Требования к отчету:
   - Титульный лист: номер и название лабораторной работы, номер варианта, Фамилия И.О., номер группы.
   - Номера заданий в отчете должны соответствовать номерам заданий в учебном пособии.
   - Допускается печать текста отчета на листе с двух сторон.

Лабораторная работа № 1

Учетные записи и авторизация в ОС MS Windows

Цель работы: Изучить типы учетных записей пользователей, ознакомиться с основными принципами управления учетными записями. Изучить основные способы авторизации пользователей.

Операционные системы: Windows XP, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012.

Теоретический материал

Теоретический материал, с которым необходимо ознакомиться:

1) Учётная запись, URL: https://dic.academic.ru/dic.nsf/ruwiki/92937.
2) Ричард Э. Смит. Аутентификация: от паролей до открытых ключей = Authentication: From Passwords to Public Keys First Edition. - М.: Вильямс, 2002. - С. 432. - ISBN 0-201-61599-1.
3) Определение типа учетной записи пользователя в Windows, URL: https://support.microsoft.com/ru-ru/help/2663817/how-to-determine-your-user-account-type-in-windows.
4) Создание учетной записи пользователя в Windows, URL: https://support.microsoft.com/ru-ru/help/13951/windows-create-user-account.
5) 5 способов добавить новую учетную запись в Windows 10, URL: https://ichip.ru/sovety/5-sposobov-dobavit-novuyu-uchetnuyu-zapis-v-windows-10-229222.
6) [Инструкция] 5 Простых способов создания учетной записи Windows 7/10, URL: https://geekhacker.ru/kak-sozdat-uchetnuyu-zapis-windows/.
7) Лекция 10: Идентификация и аутентификация, управление доступом, URL: https://www.intuit.ru/studies/courses/10/10/lecture/314.
8) ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ/ Уровни доверия к результатам идентификации, URL: https://fstec.ru/component/attachments/download/2488.
9) Обзор технологий идентификации и аутентификации, URL: https://www.aladdin-rd.ru/company/pressroom/articles/obzor_tehnologij_identifikacii_i_autentifikacii.
10) Контроль учетных записей, URL: https://docs.microsoft.com/ru-ru/windows/security/identity-protection/user-account-control/user-account-control-overview.

Основная часть

1) Дайте определение терминам: диспетчер учетных записей (SAM - Security Account Manager), монитор безопасности (SRM - Security Reference Monitor), маркер доступа (access token), идентификатор безопасности (SID - Security Identifier), привилегии пользователя, права пользователя (user rights), права пользователя, объект доступа, субъект доступа, олицетворение (impersonation), список контроля доступа (ACL - Access Control List), учетная запись, домен (*в отчете: не надо писать определения*).

2) Создайте пользователя User_№ варианта, входящего в группу «Пользователи». Опишите все способы создания, а также (на примерах) возможности данного пользователя по изменению конфигурации системы (минимум 3 примера) (*в отчете: подробное описание выполнения задания со скриншотами*).

3) Создайте администратора Admin_№ варианта, входящего в группу «Администраторы». Опишите все способы создания, а также (на примерах) ограничения данного пользователя по изменению конфигурации системы (минимум 3 примера) (*в отчете: подробное описание выполнения задания со скриншотами*).

4) Опишите параметры контроля учетных записей пользователей (UAC) (*в отчете: перечислить параметры и дать им определение*).

5) Выполните настройки механизмов защиты ОС Windows в соответствии с вариантом. Проанализируйте выполненные Вами настройки механизма защиты в части выполнения ими требований руководящих документов в области защиты информации. Сформулируйте, в чем не выполняются данные требования. Проанализируйте реализацию в ОС Windows механизма защиты в целом (не конкретно для Вашего примера) (*в отчете: подробное описание выполнения задания со скриншотами, анализ выполненных настроек, ответ на вопрос о невыполнении требований, анализ реализации в ОС*).

Варианты заданий:

1. Настроить вход пользователя в систему по паролю. Рассмотреть и реализовать возможные способы усиления парольной защиты.
2. Настроить вход пользователя в систему в безопасном режиме по паролю. Рассмотреть и реализовать возможные способы усиления парольной защиты.
3. Настроить вход пользователя в систему по смарт-карте. Обосновать целесообразность использования электронных аутентификаторов.

4. Настроить вход пользователя в систему по паролю с контроллера домена (AD - Active Directory). Рассмотреть работу механизма аутентификации при отключении контроллера домена от сети.
5. Настроить вход пользователя в систему по смарт-карте с контроллера домена (AD). Рассмотреть работу механизма аутентификации при отключении контроллера домена от сети
6. Реализовать и проиллюстрировать возможность запуска приложения под другой учетной записью после аутентификации.
7. Проиллюстрировать принадлежность в ОС Windows буфера обмена рабочему столу – одновременно нескольким пользователям.
8. Проиллюстрировать возможные причины некорректной идентификации субъекта доступа «процесс».
9. Написать программу, на которой проиллюстрировать возможности сервисов олицетворения для смены пользователя при доступе к ресурсам. Рассмотреть, в чем состоит задача аутентификации.
10. Реализовать и проанализировать возможности реализации штатными средствами ОС Windows механизма обеспечения замкнутости программной среды для корректной идентификации субъекта доступа «процесс».

Дополнительная часть

1) Опишите создание профиля пользователя и его копирование (на основе Windows Server) (*в отчете: подробное описание выполнения задания со скриншотами*).

2) Опишите настройку и работу со смарт-картами (локально и в домене) (*в отчете: подробное описание выполнения задания со скриншотами*).

3) Опишите отличия компонентов биометрической службы Windows 10 от предыдущих версий ОС (*в отчете: подробное описание выполнения задания со скриншотами*).

Контрольные вопросы

1) Перечислите типы учетных записей.
2) Перечислите способы создания учетных записей.
3) Что понимается под идентификацией пользователя?
4) Что понимается под аутентификацией пользователей?
5) Перечислите возможные идентификаторы при реализации механизма идентификации.
6) Перечислите возможные идентификаторы при реализации механизма аутентификации.
7) Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
8) Опишите механизм аутентификации пользователя.
9) Структура маркера доступа.
10) Структура SID.

Лабораторная работа №2

Разграничение доступа к объектам файловой системы

Цель работы: Изучить объекты файловой системы, ознакомиться с основными принципами управления доступом к файловым системам. Изучить основные способы настройки доступа к объектам файловой системы.

Операционные системы: Windows XP, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012.

Теоретический материал

Теоретический материал, с которым необходимо ознакомиться:

1) Обзор файловых систем FAT, HPFS и NTFS, URL: https://support.microsoft.com/ru-kz/help/100108.
2) Файлы и файловая система, URL: https://www.sites.google.com/a/i-dist.ru/informacionnye-tehnologii-ucebnoe-posobie/operacionnye-sistemy-personalnogo-komputera/fajly-i-fajlovaa-sistema.
3) Файловые системы: сравнение, секреты и уникальные особенности, URL: https://xakep.ru/2016/10/28/file-system-secrets/.
4) Файловая система, URL: http://citforum.ru/operating_systems/sos/glava_10.
5) Обзор управления доступом, URL: https://docs.microsoft.com/ru-ru/windows/security/identity-protection/access-control/access-control.
6) Лекция 13: Система управления доступом, URL: https://www.intuit.ru/studies/professional_retraining/962/courses/217/lecture/5609?page=3.
7) К.А. Щеглов, А.Ю. Щеглов, Новая технология контроля и разграничения прав доступа к данным в информационных системах, URL: http://ispdn.ru/publications/pancir.pdf.
8) Разграничение доступа к объектам в ОС Windows, URL: https://lektsii.org/9-63798.html.
9) Настройка разрешений файловой системы NTFS, URL: https://windowsnotes.ru/other/nastrojka-razreshenij-fajlovoj-sistemy-ntfs/.
10) Лекция 7: Подсистема ввода-вывода. Файловые системы, URL: https://www.intuit.ru/studies/courses/631/487/lecture/11059?page=9

Основная часть

1) Укажите минимальный набор разрешений (прав доступа), необходимых для:

a. загрузки операционной системы;
b. входа Пользователя (user_№варианта) и Администратора (admin_№варианта) в систему;
c. работы с приложениями, установленными администратором.

Разрешения указывать в форме R, W, X, в таблице:

Название объекта доступа	**Администратор**	**Пользователь**
объект доступа	*разрешения (права доступа)*	*разрешения (права доступа)*
объект доступа	*разрешения (права доступа)*	*разрешения (права доступа)*
...	...	...

2) Преобразуйте файловую систему FAT (File Allocation Table) в NTFS (New Technology File System). Опишите преобразование в отчете с использованием скриншотов (минимум 2 способа) (*в отчете: подробное описание выполнения задания со скриншотами*).

3) Выполните задание в соответствии с номером варианта, 1 – для нечетных вариантов, 2 – для четных вариантов. Для выполнения задания нужно создать файл с названием «№варианта.txt» и папку «№варианта», в которую поместить созданный файл (*в отчете: расписать права доступа, продемонстрировав на скриншотах*).

Варианты заданий:

1. Какие разрешения (права доступа) будут у Пользователя и у Администратора на файл «№варианта.txt», если владельцем файла является Администратор, для Пользователя установлено разрешение «Запись» («Write»), для Администратора установлено разрешение «Чтение» («Read»), а для группы «Все» («Everyone») (оба пользователя входят в эту группу) - разрешение «Изменение» («Change»)?
2. Какие разрешения (права доступа) будут у Пользователя и у Администратора на файл «№варианта.txt», если владельцем папки «№варианта» является Пользователь, для пользователя установлено

разрешение «Чтение» («Read»), для Администратора установлено разрешение «Полный доступ» («Full control»), а для группы «Все» («Everyone») (оба пользователя входят в группу) – не установлены разрешения (установлено «No Access»)?

4) Выполните задание в соответствии с номером варианта, номер задания соответствует второй цифре номера варианта (например, 40 вариант – 10 задание, 34 вариант – 4 задание и т.п.). Выполните настройки встроенных механизмов защиты ОС Windows в соответствии с заданием (*в отчете: подробное описание настроек встроенных механизмов защиты и выполненных действий со скриншотами*).

Варианты заданий:

1. Разрешить встроенными средствами ОС Windows пользователю запускать исполняемые файлы из папки «Program Files», запретить возможность её модификации. Проанализировать возможность и сложность настройки.
2. Разрешить встроенными средствами ОС Windows только пользователю System запуск процессов из системного диска. Предотвратить возможность его модификации. Проанализировать возможность и сложность настройки.
3. Запретить встроенными средствами ОС Windows пользователю запись информации на внешние flash-накопители. Проанализировать возможность и сложность настройки.
4. Запретить встроенными средствами ОС Windows пользователю запуск программ с внешних flash-накопителей. Проанализировать возможность и сложность настройки.
5. Запретить встроенными средствами ОС Windows пользователю запуск программ из сети (с разделенных в сети файловых объектов). Проанализировать возможность и сложность настройки.
6. Проиллюстрировать невозможность разделения встроенными средствами ОС Windows между пользователями некоторых объектов из папки «All users».
7. Завести папку для хранения данных, разрешить встроенными средствами ОС Windows доступ пользователя к этой папке с данными, предотвратить возможность её переименования и создание новых папок для хранения данных. Остальным пользователям доступ к этой папке запретить. Проанализировать возможность и сложность настройки.

8. Разрешить встроенными средствами ОС Windows доступ пользователя только к одной папке с данными, предотвратить возможность её переименования и создание новых папок для хранения данных. Остальным пользователям доступ к этой папке запретить. Проанализировать возможность и сложность настройки.
9. Завести файл на диске для хранения данных, разрешить встроенными средствами ОС Windows доступ пользователя к этому файлу с данными, предотвратить возможность его переименования и создание новых файлов для хранения данных. Остальным пользователям доступ к этому файлу запретить встроенными средствами ОС Windows. Проанализировать возможность и сложность настройки.
10. Разрешить встроенными средствами ОС Windows доступ пользователя только к одному файлу с данными, предотвратить возможность его переименования и создание новых файлов для хранения данных. Остальным пользователям доступ к этому файлу запретить. Проанализировать возможность и сложность настройки.
11. Запретить запуск приложений, начинающихся на символ «D», из домашних каталогов пользователей. Проанализировать возможность и сложность настройки.

5) Разрешите средствами операционной системы выполнять системные и прикладные программы только из папок %ProgramFiles% и %SystemRoot% (*в отчете: подробное описание выполнения задания со скриншотами*).

Дополнительная часть

1) Опишите на примерах работу с разрешениями NTFS дополнительных системных программ сторонних производителей (*в отчете: описание работы всех программ со скриншотами*). Приведите перечень подобных программ (не менее пяти).

2) Сравните файловые системы FAT и NTFS (*в отчете: сравнение выполнить в виде таблицы*).

3) Опишите все возможные способы задания разрешений (прав доступа) к файлам и папкам (*в отчете: подробное описание выполнения задания со скриншотами*).

Контрольные вопросы

1) Что такое файловая система?
2) Перечислите существующие файловые системы.
3) Какова модель разграничения доступа в ОС Windows?
4) Что такое DACL?
5) Перечислите существующие разрешения для пользователей.
6) Расскажите про наследование разрешений.
7) Перечислите способы для разграничения доступа.
8) В чем отличие между пользовательскими и системными переменными окружения?
9) Перечислите три достоинства FAT.
10) Перечислите три недостатка NTFS.

Лабораторная работа №3

Разграничение доступа к реестру

Цель работы: Изучить объекты реестра, ознакомиться с основными принципами управления доступом к объектам реестра. Изучить основные способы настройки доступа к реестру.

Операционные системы: Windows XP, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012.

Теоретический материал

Теоретический материал, с которым необходимо ознакомиться:

1) Сведения о реестре Windows для опытных пользователей, URL: https://support.microsoft.com/ru-ru/help/256986.
2) Прямой распил реестра Windows, URL: https://xakep.ru/2013/08/22/61122/.
3) Что такое реестр Windows 10/8/7?, URL: http://it-uroki.ru/uroki/opytnyj-polzovatel/chto-takoe-reestr-windows.html.
4) Архитектура системного реестра Windows. Часть 1, URL: http://www.interface.ru/home.asp?artId=35994.
5) Основные ключи реестра Microsoft Windows, URL: https://www.chemtable.com/blog/ru/windows-registry-main-keys.htm.

Основная часть

1) Какие конкретно ветки и ключи доступны (*в отчёте: перечислите их названия*):
   a) Пользователю хотя бы на чтение;
   b) только Администратору;
   c) только System.

2) Опишите в отчете способы резервного копирования реестра (**для четных вариантов**) (*в отчете: подробное описание выполнения задания со скриншотами*).

3) Опишите в отчете способы восстановления реестра (**для нечетных вариантов**) (*в отчете: подробное описание выполнения задания со скриншотами*).

4) Данное задание выполняется исходя из варианта. Укажите ключ, который отвечает за указанный параметр системы (*в отчете: подробное описание выполнения задания со скриншотами).* Ответ на данное задание **прислать** на электронный адрес преподавателя **минимум** за **трое** суток до сдачи данной лабораторной работы.

Варианты заданий:

Вариант 1:

a. Переход системы в гибернацию.
b. Отключение запроса пароля при выходе из ждущего режима.
c. Отключение сообщения об ошибках на странице и их отладка в Internet Explorer (Microsoft Edge).

Вариант 2:

a. Настройка службы Superfetch: включение механизма Prefetcher.
b. Отключение всплывающей подсказки.
c. Блокировка кнопок «Вперед» и «Назад» в Internet Explorer (Microsoft Edge).

Вариант 3:

a. Настройка службы Superfetch: включение механизма Prefetcher только для загрузки системы.
b. Автозагрузка Microsoft Office Word при запуске системы.
c. Отображение мелких значков в меню «Пуск».

Вариант 4:

a. Настройка службы Superfetch: включение механизма Prefetcher во время работы и при загрузке системы.
b. Отключение автоматического обновления системы.
c. Отключение записи последнего времени доступа к файлам.

Вариант 5:

a. Настройка службы Superfetch: отключение трассировки службы.
b. Изменение заставки.
c. Ускорение открытия меню «Пуск».

Вариант 6:

a. Задание классического вида панели управления.
b. Отображение пароля к сетевым ресурсам.
c. Автоматическое завершение всех приложений при выключении компьютера.

Вариант 7:

a. Настройка службы Superfetch: включение службы Superfetch.
b. Отключение истории списка последних и часто используемых файлов.
c. Отключение вызова диспетчера задач.

Вариант 8:

a. Настройка службы Superfetch: включение службы Superfetch только для загрузки системы.
b. Отключение выделения недавно установленных программ.
c. Изменение задержки предварительного просмотра панели задач.

Вариант 9:

a. Настройка службы Superfetch: включение службы Superfetch во время работы, но при этом чтобы была отключена при загрузке системы.
b. Сортировка меню по алфавиту.
c. Установка версии Windows на рабочем столе.

Вариант 10:

a. Включение доступа к настройкам DVD в Windows Media Player.
b. Отключение добавления окончания "- ярлык" к названию ярлыков при их создании.
c. Запрет отображения раздела «Недавние Документы» в меню «Пуск».

Вариант 11:

a. Настройка службы Superfetch: включение службы Superfetch во время работы и при загрузке системы.
b. Удаление пункта «Справка».
c. Удаление пункта «Выход из системы».

Вариант 12:

a. Отключение кэширования изображений.
b. Отключение автозапуска CD/DVD-дисков.
c. Запрет на выгрузку из оперативной памяти кодов ядра и драйверов.

Вариант 13:

a. Выгрузка из памяти неиспользуемых DLL.
b. Переименование «Корзину». Измените её название.
c. Запрет на попадание приложения в список часто используемых программ.

Вариант 14:

a. Удаление стрелки с ярлыков.
b. Ограничение удаленного доступа к реестру определенного компьютера.
c. Скрытие учетной записи.

Вариант 15:

a. Запрет выгрузки из оперативной памяти кодов ядра.
b. Очищение файла подкачки при выключении компьютера.
c. Отключение создания специальной таблицы файлов для имен в формате MS-DOS.

Вариант 16:

a. Отключение появления любых сообщений в нижнем правом углу (о подключении к интернету, локальной сети и др.).
b. Отключение сообщения о просмотре вэб-страницы через безопасное соединение.
c. Ускорение открытия видео в формате AVI.

Вариант 17:

a. Очистка истории введенных адресов в (Internet Explorer) Microsoft Edge.
b. Отключение сообщения в браузере «Информация, передаваемая через Интернет, может стать доступной другим пользователям».
c. Отключение восстановления системы.

Вариант 18:

a. Запрет создания таблицы совместимости со старыми приложениями в разделе NTFS.
b. Включение ускоренной перезагрузки.
c. Отключение автозагрузки со всех типов носителей.

Вариант 19:

a. Изменение информации о зарегистрированном владельце копии Windows.
b. Отключение POSIX.
c. Деактивация клавиши «Win».

Вариант 20:

a. Отображение значков в меню «Пуск» мелкими.
b. Отключение метки последнего доступа к файлам для разделов NTFS.
c. Автоматическое закрытие без всякого предупреждения всех зависших программ.

Вариант 21:

a. Отображение значков в меню «Пуск» крупными.
b. Требование пароля только из букв и цифр.
c. Отмена сохранения информации о подключенных USB-устройствах.

Вариант 22:

a. Скрытие/отображение пользователей в диалоговом окне входа в систему.
b. Изменение задержки предварительного просмотра панели задач.
c. Отключение отправки отчетов об ошибках в MS Office.

Вариант 23:

a. Создание псевдонимов к программам.
b. Отсутствие разрыва связи при выходе из системы.
c. Автоматическое удаление временных файлов после работы в Интернет.

Вариант 24:

a. Отображение версии Windows в правом нижнем углу экрана.
b. Установка минимального количества символов в паролях.
c. Уничтожение при завершении работы всей информации, которая могла сохраниться в системном файле Page File.

Вариант 25:

a. Запрет отображения напоминания Outlook Express.
b. Отмена сохранения списка документов, с которыми вы работали.
c. Увеличение числа страниц, которые система будет читать или писать на жесткий диск за один раз.

Вариант 26:

a. Изменение раскладки клавиатуры при входе в систему.
b. Включение режима, при котором в режиме обзора сети другие пользователи не будут видеть вашего компьютера.
c. Отключение вызова диспетчера задач.

Вариант 27:

a. Отключение функции слежения за действиями пользователя, включая запускаемые программы и открываемые документы.
b. Установка размера кэша, резервируемого для CD-ROM.
c. Удаление значка «Корзина» с рабочего стола.

Вариант 28:

a. Запрет использования REGEDIT.EXE.
b. Отключение кэширования паролей.
c. Добавление кнопки «Музыка» на панели команд Проводника.

Вариант 29:

a. Изменение порога выдачи предупреждения о недостатке свободного места на диске.
b. Добавление значка «Корзина» в «Мой компьютер».
c. Отключение поиска сетевых принтеров.

Вариант 30:

a. Настройку службы Superfetch: включение механизма Prefetcher во время работы, но при этом чтобы была отключена при загрузке системы.
b. Повышение приоритета активным приложениям.
c. Изменение фонового рисунка экрана входа Windows LogOn.

Вариант 31:

a. Отключение появления любых сообщений в нижнем правом углу (о подключении к интернету, локальной сети и др.).
b. Отключение сообщения о просмотре вэб-страницы через безопасное соединение.
c. Ускорение открытия видео в формате AVI.

Вариант 32:

a. Очистка истории введенных адресов в (Internet Explorer) Microsoft Edge.
b. Отключение сообщения в браузере «Информация, передаваемая через Интернет, может стать доступной другим пользователям».
c. Отключение восстановления системы.

Вариант 33:

a. Запрет создания таблицы совместимости со старыми приложениями в разделе NTFS.
b. Включение ускоренной перезагрузки.
c. Отключение автозагрузки со всех типов носителей.

Вариант 34:

a. Изменение информации о зарегистрированном владельце копии Windows.
b. Отключение POSIX.
c. Деактивация клавиши «Win».

Вариант 35:

a. Отображение значков в меню "Пуск" мелкими.
b. Отключение метки последнего доступа к файлам для разделов NTFS.
c. Автоматическое закрытие без всякого предупреждения всех зависших программ.

Вариант 36:

a. Отображение значков в меню «Пуск» крупными.
b. Требование пароля только из букв и цифр.
c. Отмена сохранения информации о подключенных USB-устройствах.

Вариант 37:

a. Скрытие/отображение пользователей в диалоговом окне входа в систему.
b. Изменение задержки предварительного просмотра панели задач.
c. Отключение отправки отчетов об ошибках в MS Office.

Вариант 38:

a. Создание псевдонимов к программам.
b. Отсутствие разрыва связи при выходе из системы.
c. Очистка истории введенных адресов в Internet Explorer (Microsoft Edge).

Вариант 39:

a. Отображение версии Windows в правом нижнем углу экрана.
b. Установка минимального количества символов в паролях.
c. Уничтожение при завершении работы всей информации, которая могла сохраниться в системном файле Page File.

Вариант 40:

a. Запрет отображения напоминания Outlook Express.
b. Отмену сохранения списка документов, с которыми вы работали.
c. Увеличение числа страниц, которые система будет читать или писать на жесткий диск за один раз.

Вариант 41:

a. Изменение раскладки клавиатуры при входе в систему.
b. Включение режима, при котором в режиме обзора сети другие пользователи не будут видеть вашего компьютера.
c. Отключение вызова диспетчера задач.

Вариант 42:

a. Запрет использования REGEDIT.EXE.
b. Отключение кэширования паролей.
c. Добавление кнопки «Музыка» на панели команд Проводника.

Вариант 43:

a. Изменение порога выдачи предупреждения о недостатке свободного места на диске.
b. Добавление значка «Корзина» в «Мой компьютер».
c. Отключение поиска сетевых принтеров.

Вариант 44:

a. Настройка службы Superfetch: включение механизма Prefetcher во время работы, но при этом чтобы была отключена при загрузке системы.
b. Повышение приоритета активным приложениям.
c. Изменение фонового рисунка экрана входа Windows LogOn.

Вариант 45:

a. Отключение появления любых сообщений в нижнем правом углу (о подключении к интернету, локальной сети и др.).
b. Отключение сообщения о просмотре вэб-страницы через безопасное соединение.
c. Ускорение открытия видео в формате AVI.

Вариант 46:

a. Очистка истории введенных адресов в Internet Explorer (Microsoft Edge)
b. Отключение сообщения в браузере "Информация, передаваемая через Интернет, может стать доступной другим пользователям".
c. Отключение восстановления системы.

Вариант 47:

a. Запрет создания таблицы совместимости со старыми приложениями в разделе NTFS.
b. Включение ускоренной перезагрузки.
c. Отключение автозагрузки со всех типов носителей.

Вариант 48:

a. Изменение информации о зарегистрированном владельце копии Windows.
b. Включение автоматического открытия папок после загрузки системы, если они не были закрыты пользователем перед перезагрузкой.
c. Деактивация клавиши «Win».

Вариант 49:

a. Настройка службы Superfetch: включение механизма Prefetcher только для загрузки системы.
b. Автозагрузка Microsoft Office Word при запуске системы.
c. Отображение мелких значков в меню «Пуск».

Вариант 50:

a. Настройка службы Superfetch: включение механизма Prefetcher во время работы и при загрузке системы.
b. Отключение автоматического обновления системы.
c. Отключение записи последнего времени доступа к файлам.

Вариант 51:

a. Настройка службы Superfetch: отключение трассировки службы.
b. Изменение заставки.
c. Отключение добавления приставки "Ярлык для" к названию ярлыков при их создании.

Вариант 52:

a. Задание классического вида панели управления.
b. Отображение пароля к сетевым ресурсам.
c. Автоматическое завершение всех приложений при выключении компьютера.

Вариант 53:

a. Настройка службы Superfetch: включение службы Superfetch.
b. Отключение истории списка последних часто и используемых файлов.
c. Отключение вызова диспетчера задач.

Вариант 54:

a. Настройка службы Superfetch: включение службы Superfetch только для загрузки системы.
b. Отключение выделения недавно установленных программ.
c. Изменение задержки предварительного просмотра панели задач.

Вариант 55:

a. Настройка службы Superfetch: включение службы Superfetch во время работы, но при этом чтобы была отключена при загрузке системы.
b. Сортировка меню по алфавиту.
c. Включение доступа к настройкам DVD в Windows Media Player.

5) Настройте на аудит какую-либо ветку реестра и проследите появление событий (минимум 5 подразделов) (*в отчете: подробное описание выполнения задания со скриншотами*).

6) Приведите примеры аналогов Regedit. Приведите плюсы и минусы по сравнению с Regedit (минимум 3) (*в отчете: примеры со скриншотами, описание*)

Дополнительная часть

1) При помощи Process Monitor для какой-либо программы (notepad, wordpad или другой текстовый редактор) установите адрес хранения настроек (размер шрифта, имя шрифта и т.п.) в реестре. Попробуйте поменять настройки через реестр вручную, проследите и отобразите в отчете реакцию программы (*в отчете: подробное описание выполнения задания со скриншотами*).

2) Напишите программу аналог Regedit. Должна быть реализована возможность просмотра всех параметров, их редактирование (*в отчете: исходный код и интерфейсы*).

Контрольные вопросы

1) Что такое реестр?
2) Как запустить редактор реестра?
3) Как сохранить реестр перед редактированием?
4) Как восстановить реестр?
5) Расскажите о структуре реестра.
6) Из каких файлов состоит реестр? Где они расположены?
7) Расскажите о назначении реестра.
8) Назовите ключи, имеющие псевдонимы.
9) Расскажите о способах редактирования реестра.
10) Назовите основные разделы и их назначение.

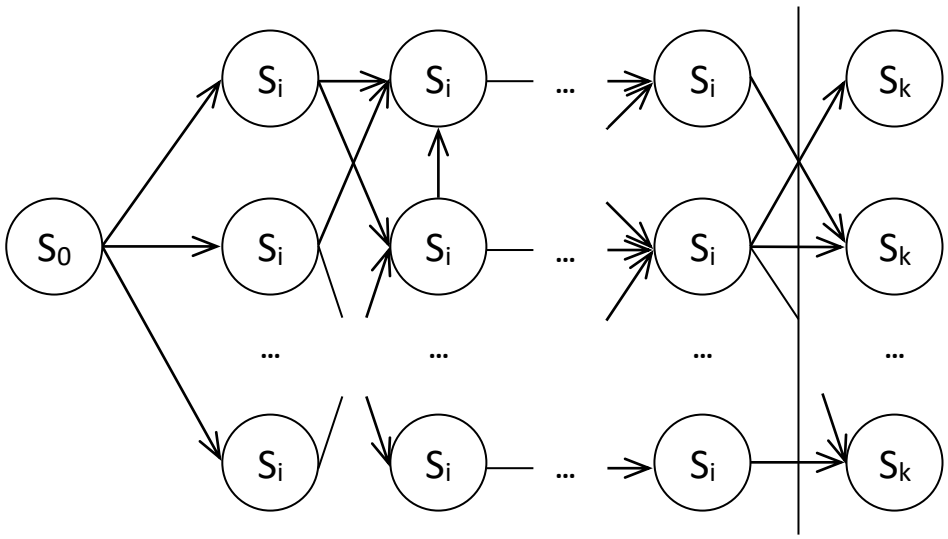
Лабораторная работа №4

Основная часть

Необходимо сделать доклад об одной из компьютерных атак на выбор. Тема доклада не должна повторяться среди студентов одного потока. Доклад должен в себя включать подробное описание последовательности действий злоумышленника с примерами.

Действия злоумышленника следует представить в виде орграфа. В графе должны быть обязательно исходное состояние системы (S_0), в котором злоумышленник бездействует, и конечные состояния (S_k), такие как кража информации, модификация информации, отказ в доступе и др.

На рисунке представлен пример подобного орграфа.



На рисунке:

S_0 – исходное состояние системы без воздействия злоумышленника;

S_i – состояние системы, которое выражает действие злоумышленника либо состояние информационной системы.

S_k – конечное состояние системы, характеризуемое потерей от осуществления атаки; в общем случае имеются в виду следующие потери: модификация или удаление информации, кража информации, отказ в обслуживании или доступе.

Предлагаемые типы атак:

- использование специальных программ (вирусы, снифферы и др.);
- прослушивание (Eavesdropping);
- фишинг;
- сниффинг пакетов в локальной сети;
- Tride flood Network;
- полный перебор паролей;
- Drive-by атаки;
- Ip-спуффинг;
- DDos (Denial of Service);
- XSS (Cross-Site Scripting);
- SQL-Injection;
- Mail-bombing;
- DNS Cache Poisoning (Атака Каминского);
- Padding Oracle;
- CSRF (Cross Site Request Forgery);
- переполнение буфера;
- MITM (Man in the Middle);
- Bad connect/Pipes/Reverse (Обратный сеанс);
- атаки на WebProxy с использованием DNS и WINS сервера;
- фиксация сессии;
- социальная инженерия;
- получение доступа к сети LTE;
- атака нулевого дня;
- взлом IIS сервера (основные уязвимости);
- Dummy DNS Server (ложный DNS Сервер);
- навязывание хосту ложного маршрута с использованием протокола ICMP;
- атака на функции форматирования строк (Format String Attack).

Предлагаемый список не является полным. Можно взять другие типы атак, которые Вам наиболее интересны.

Рекомендуемая литература и ресурсы сети Интернет

1. Центр безопасности Microsoft Windows https://msdn.microsoft.com/ru-ru/security/default
2. Ресурс компании Microsoft по администрированию, виртуализации, облачным вычислениям https://technet.microsoft.com/ru-ru/
3. Лекция 15: Отдельные аспекты безопасности Windows. Основы организации операционных систем Microsoft Windows. // НОУ ИНТУИТ, http://www.intuit.ru/studies/courses/1089/217/lecture/5613
4. Лекция 16: Защитные механизмы операционных систем. Основы операционных систем. // НОУ ИНТУИТ, http://www.intuit.ru/studies/courses/2192/31/lecture/998
5. Уильям Р. Станек. Windows 7 для продвинутых // Издательство: Питер Год: 2011
6. Чекмарев А.Н. Microsoft Windows Server 2008 (в подлиннике) Издательство: БХВ-Петербург Год: 2008
7. Бэллью Дж., Дантеман Дж. Зачищаем Windows, или как значительно ускорить работу компьютера, очистив его от накопившегося хлама Издательство: Символ-Плюс Год: 2008
8. Колисниченко Д.Н. Секреты, настройка и оптимизация реестра Windows 7 Издательство: БХВ-Петербург Год: 2010
9. Jordan Krause Windows Server 2012 R2 Administrator Cookbook Издательство: Packt Publishing Год: 2015
10. Рэнд Моримото, Майкл Ноэл, Гай Ярдени, Омар Драуби, Эндрю Аббат, Крис Амарис Microsoft Windows Server 2012. Полное руководство Издательство: Вильямс Год: 2013
11. Уильям Р. Станек Microsoft Windows 8. Справочник администратора Издательство: БХВ-Петербург Год: 2014
12. Уильям Р. Станек Windows 7. Справочник администратора Издательство: Русская Редакция, БХВ-Петербург Год: 2010
13. Кокорева О. Реестр Windows 7 Издательство: БХВ-Петербург Год: 2010
14. Уильям Р. Станек Windows Server 2008. Справочник администратора Издательство: БХВ-Петербург Год: 2008
15. Чекмарев А. Н. Microsoft Windows 7. Руководство администратора Издательство: БХВ-Петербург Год: 2010
16. Руссинович М., Маргозис А. Утилиты Sysinternals. Справочник администратора Издательство: Русская редакция, БХВ-Петербург Год: 2012
17. Дэвид Карп Хитрости Windows 7. Для профессионалов Издательство: Питер Год: 2011

18. Белозубов А.В., Билевич С.А., Николаев Д.Г. Основы работы в Windows7. Издательство: СПб.: СПбГУ ИТМО Год: 2011
19. Климов А. П. Реестр Windows 7 Издательство: Питер Год: 2010
20. Рэнд Моримото, Майкл Ноэл, Омар Драуби, Росс Мистри, Крис Амарис Microsoft Windows Server 2008 R2. Полное руководство Издательство: Вильямс Год: 2011

Маркина Татьяна Анатольевна

Основные механизмы защиты в ОС MS Windows. Методические рекомендации по выполнению лабораторных работ

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверский пр., 49