УНИВЕРСИТЕТ ИТМО

Т.А. Маркина

Основные механизмы защиты в ОС MS Windows.

Методические рекомендации

по выполнению лабораторных работ

Учебно-методическое пособие

Санкт-Петербург
2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

Т.А. Маркина

Основные механизмы защиты в ОС MS Windows.

Методические рекомендации по выполнению лабораторных работ

Учебно-методическое пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург

2015

Маркина Т.А. Основные механизмы защиты в ОС MS Windows. Методические рекомендации по выполнению лабораторных работ. Учебно-методическое пособие. – СПб: Университет ИТМО, 2015. – 48 с.

Пособие содержит теоретический минимум, методические указания и задания для выполнения лабораторных работ по дисциплине «Безопасность вычислительных систем и сетей». Пособие предназначено для магистров направления подготовки 09.04.01 «Информатика и вычислительная техника».

Рекомендовано к печати Ученым советом факультета компьютерных технологий и управления, протокола № 6 от 23 июня 2015 г.

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.

© Университет ИТМО, 2015

©Т.А. Маркина, 2015

Содержание

Введение

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.

В рамках курса рассматриваются защитные механизмы и компоненты безопасности операционных систем Windows XP, Windows 7, Windows 8, Windows Server 2008 R2 и Windows Server 2012.

Особое внимание уделено практическим работам, иллюстрирующим возможности систем безопасности операционных систем MS Windows.

Правила проведение лабораторных работ и требования к отчетности

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. Содержание отчета:
   - цель работы;
   - программно-аппаратные средства, 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).
6. 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 задании.

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.

Краткий теоретический материал

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:

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

По способу авторизации можно выделить две группы:

- локальная учетная запись;
- 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:

- Создание учетных записей пользователей для компьютеров, состоящих в рабочей группе:
  - Создание учетной записи при помощи диалога «Управление учетными записями пользователей».
  - Создание учетной записи при помощи диалога «Учетные записи пользователей».
  - Создание учетной записи при помощи оснастки «Локальные пользователи и группы».
  - Создание учетной записи при помощи командной строки (команда net user).

- Создание учетных записей пользователей для компьютеров, состоящих в домене:
  - Создание пользователей при помощи оснастки «Active Directory – пользователи и компьютеры».
  - Создание пользователей с помощью командной строки (команда dsadd user).
  - Импорт пользователей с помощью команды CSVDE.
  - Импорт пользователей с помощью команды LDIFDE.
  - Создание пользователей с помощью Windows PowerShell.
  - Создание пользователей с помощью VBScript.

Для того чтобы произвести изменения в учетный записей, 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.

Идентификация – процедура распознавания субъекта по его уникальному идентификатору, присвоенному данному субъекту ранее и занесенному в базу данных в момент регистрации субъекта в качестве легального пользователя системы.

Аутентификация – процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор. В зависимости от степени доверительных отношений, структуры, особенностей сети и удаленностью объекта проверка может быть односторонней или взаимной. В большинстве случаев она состоит в процедуре обмена между входящим в систему объектом и ресурсом, отвечающим за принятие решения ("да" или «нет»). Данная проверка, как правило, производится с применением криптографических преобразований, которые нужны, с одной стороны, для того, чтобы достоверно убедиться в том, что субъект является тем, за кого себя выдает, с другой стороны − для защиты трафика обмена субъект система от злоумышленника. Таким образом, идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности пользователей.

Именно от корректности решения этих двух задач (распознавания и проверки подлинности) зависит, можно ли разрешить доступ к ресурсам системы конкретному пользователю, т.е. будет ли он авторизован.

В частных и государственных компьютерных сетях (включая Интернет) наиболее часто для аутентификации предполагается проверка учетных данных пользователя, то есть, имя пользователя и пароль. Однако для типов критических транзакций, например обработка платежей, проверки подлинности имени пользователя и пароля не достаточно, так как пароли могут быть украдены или взломаны. По этой причине, основная часть интернет-бизнеса, а также многие другие сделки теперь

используют цифровые сертификаты, которые выдаются и проверяются центром сертификации.

Авторизация – процедура предоставления субъекту определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к её ресурсам.

Операционная система Windows 7 для входа в сеть имеет следующие методы аутентификации:

- Протокол Kerberos версии 5: Основной метод аутентификации клиентов и серверов под управлением операционных систем Microsoft Windows. Он используется для проверки подлинности учетных записей пользователей и учетных записей компьютеров.
- Windows NT LAN Manager (NTLM): используется для обратной совместимости с операционными системами более старыми, чем Windows 2000 и некоторых приложений. Он менее гибок, эффективен и безопасен, чем протокол Kerberos версии 5.
- Сопоставление сертификатов: обычно используется для проверки подлинности при входе в сочетании со смарт-картой. Сертификат, записанный на смарт-карте, связан с учетной записью пользователя. Для чтения смарт-карт и аутентификации пользователя используется считыватель смарт-карт.
- Биометрия.

Контроль учётных записей пользователей (англ. User Account Control, UAC) – компонент операционных систем Microsoft Windows, впервые появившийся в Windows Vista. Этот компонент запрашивает подтверждение действий, требующих прав администратора, в целях защиты от несанкционированного использования компьютера. Администратор компьютера может отключить Контроль учётных записей пользователей в Панели управления.

Основная часть

1) Изучите теоретический материал лабораторной работы. Знать определения: диспетчер учетных записей (SAM), монитор безопасности (SRM), маркер доступа (access token), идентификатор безопасности (SID), привилегии пользователя, права пользователя (user rights), права пользователя, объект доступа, субъект доступа, олицетворение (impersonation), список контроля доступа (ACE), учетная запись, домен.

2) Создайте пользователя User_№ варианта, входящего в группу «Пользователи». Опишите на примерах возможности данного пользователя по изменению конфигурации системы (3 примера, скриншоты).

3) Создайте администратора Admin_№ варианта, входящего в группу «Администраторы». Опишите на примерах ограничения данного пользователя по изменению конфигурации системы (3 примера, скриншоты).

4) Опишите параметры контроля учетных записей пользователей (UAC). (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). Сформулируйте, в чем не выполняются данные требования

Варианты заданий (вариант необходимо получить у преподавателя):

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). 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 (повышенная сложность).
10. Реализовать и проанализировать возможности реализации штатными средствами ОС Windows механизма обеспечения замкнутости программной среды для корректной идентификации субъекта доступа процесс (повышенная сложность).

Дополнительное задание

1) Описать создание профиля пользователя и его копирование (на основе Windows Server 2008 или Windows Server 2012) (скриншоты).

2) Описать настройку и работу со смарт-картами (локально и в домене).

3) Описать компоненты биометрической службы. (Перечислить компоненты и дать им описание.)

Лабораторная работа №2

Разграничение доступа к объектам файловой системы

Краткий теоретический материал

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:

- NTFS – основная файловая система семейства Windows NT;
- 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;
- exFAT (Extended FAT – расширенная FAT) – развитие файловой системы FAT, использующее 64 разрядные идентификаторы. Применяется в основном для устройств флеш-памяти;
- CDFS (CD ROM File System) – файловая система для CD дисков, объединяющая форматы ISO 96601 и Joliet2;

- 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:

- обзор папок (выполнение файлов);
- содержание папки (чтение данных из файла);
- чтение атрибутов;
- чтение дополнительных атрибутов;
- создание файлов (запись данных в файл);
- создание папок (дозапись данных в файл);
- запись атрибутов;
- запись дополнительных атрибутов;
- 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;

- удаление;
- чтение разрешений;
- смена разрешений;
- смена владельца;
- 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:

- *полный доступ* – пользователь, принадлежащий к указанной группе, может выполнять любые операции над папкой;
- *изменить* – означает возможность модификации файлов или

папки, в зависимости от того, чем является защищаемый объект;

- *чтение и выполнение* – возможность чтения и исполнения файлов папки;
- *список содержимого папки* – доступ к списку содержимого папки;
- *чтение* – доступ на чтение содержимого папки;
- *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;
- *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:

- Вкладка «Безопасность» в свойствах файла или папки.
- Системная утилита icacls.exe.
- Файловый менеджер.
- Средства защиты информации от несанкционированного доступа.

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:

1. перейти во вкладку Действующие разрешения окна Дополнительные параметры безопасности и нажать кнопку «Выбрать»;
2. в появившемся новом окне нажать кнопку «Типы объектов»;
3. из списка выбрать объект (Пользователь, Группа) и нажать кнопку «ОК»;
4. в окне «Выбор»: Пользователь или группа нажать кнопку «Дополнительно»;
5. появится новое окно «Выберите тип объекта»;
6. нажать кнопку «Поиск»;
7. из раскрывшегося списка выбрать пользователя или группу и нажать «ОК»;
8. появится окно с выбранным объектом, нажать кнопку «ОК»;

9. появится список действующих разрешений для выбранного пользователя или выбранной группы.

Основная часть

1) Указать минимальный набор разрешений (прав доступа) необходимых для загрузки операционной системы и входа Пользователя (user_№варианта) и Администратора (admin_№варианта) в систему и работы с приложениями, установленными администратором. Разрешения указывать R, W, X, в виде таблицы вида:

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 в NTFS. Опишите преобразование в отчете с использованием скриншотов (минимум 2 способа).

3) Выполнить задание исходя из 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. Расписать права доступа, продемонстрировав на скриншотах.

Варианты заданий (вариант необходимо получить у преподавателя):

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) Выполнить задание исходя из 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 отразите описание настроек встроенных механизмов защиты и выполненных действий.

Варианты заданий (вариант необходимо получить у преподавателя):

1. Разрешите встроенными средствами ОС Windows пользователю запускать исполняемые файлы из папки «Program Files», запретите возможность её модификации. Проанализируйте возможность и сложность настройки.
2. Разрешите встроенными средствами ОС Windows только пользователю System запуск процессов из системного диска. Предотвратите возможность его модификации. Проанализируйте возможность и сложность настройки.
3. Запретите встроенными средствами ОС Windows пользователю запись информации на внешние flash-накопители. Проанализируйте возможность и сложность настройки.

4. Запретите встроенными средствами ОС Windows пользователю запуск программ с внешних flash-накопителей. Проанализируйте возможность и сложность настройки.
5. Запретите встроенными средствами ОС Windows пользователю запуск программ из сети (с разделенных в сети файловых объектов). Проанализируйте возможность и сложность настройки.
6. Проиллюстрируйте невозможность разделения встроенными средствами ОС Windows между пользователями некоторых объектов из папки «All users».
7. Заведите папку для хранения данных, разрешите встроенными средствами ОС Windows доступ пользователя к этой папке с данными, предотвратите возможность её переименования, создание новых папок для хранения данных. Остальным пользователям доступ к этой папке запретите. Проанализируйте возможность и сложность настройки.
8. Разрешите встроенными средствами ОС Windows доступ пользователя только к одной папке с данными, предотвратите возможность её переименования, создание новых папок для хранения данных. Остальным пользователям доступ к этой папке запретите. Проанализируйте возможность и сложность настройки.
9. Заведите файл на диске для хранения данных, разрешите встроенными средствами ОС Windows доступ пользователя к этому файлу с данными предотвратите возможность его переименования создание новых файлов для хранения данных. Остальным пользователям доступ к этому файлу запретите встроенными средствами ОС Windows. Проанализируйте возможность и сложность настройки.

10. Разрешите встроенными средствами ОС Windows доступ пользователя только к одному файлу с данными предотвратите возможность его переименования, создание новых файлов для хранения данных. Остальным пользователям доступ к этому файлу запретите. Проанализируйте возможность и сложность настройки.

5) Разрешить средствами операционной системы выполнять системные и прикладные программы только из папок %ProgramFiles% и %SystemRoot% (описать процесс в отчете).

Дополнительная часть

1) Описать на примерах работу с разрешениями NTFS дополнительных системных программ сторонних производителей (отразить описание работы всех программ в отчете со скриншотами). Привести перечень подобных программ (не менее пяти).

2) Сравнить файловые системы FAT и NTFS (сравнение выполнить в виде таблицы).

3) Описать все возможные способы задания разрешений (прав доступа) к файлам и папкам.

Лабораторная работа №3

Разграничение доступа к реестру

Краткий теоретический материал

Реестр или *системный реестр* – это база данных для хранения сведений о конфигурации компьютера и настроек операционной системы.

Все декларированные, а также не декларированные возможности ОС, в том числе, те из них, которые не могут быть настроены с использованием графического пользовательского интерфейса (GUI), могут быть конфигурированы посредством Реестра. Любое запускаемое в системе приложение не может быть выполнено без обращения к Реестру, поскольку именно там находятся все его параметры.

Реестр содержит данные, к которым Windows постоянно обращается во время загрузки, работы и её завершения, а именно:

- профили всех пользователей, то есть их настройки;
- конфигурация оборудования, установленного в операционной системе.
- данные об установленных программах и типах документов, создаваемых каждой программой;
- свойства папок и значков программ;
- данные об используемых портах.

Основными элементами структуры Реестра ОС являются ключи. Каждый ключ может иметь набор параметров, каждому из которых соответствует определенное значение, а также подключи – подчиненные ключи более низкого уровня. По отношению к друг другу ключи и подключи организуются в системном Реестре в соответствии с отношением вида «предок-потомок».

Иерархическая структура Реестра ОС представляет собой дерево ключей, организованное в виде кустов или ульев (каждый из которых является двоичным файлом, называемым файлом куста), напоминающей

структуру файлов и папок файловой системы (ФС). Корневой ключ (вершина дерева) и подключи по аналогии с ФС можно считать папками, а параметры Реестра – файлами, соответственно.

Для работы с реестром используется простая и понятная утилита Regedit.

Реестр Windows XP состоит из следующих основных разделов:

Раздел реестра	**Краткое описание**
HKEY_CLASSES_ROOT (HKCR)	Это ссылка на раздел HKEY_LOCAL_MACHINE\Software\Classes. Хранящиеся здесь сведения обеспечивают запуск необходимой программы при открытии файла с помощью проводника. Этот раздел содержит связи между приложениями и типами файлов, а также информацию об OLE.
HKEY_CURRENT_USER (HKCU)	Это ссылка на определённый подраздел HKEY_USERS. Настройки соответствуют текущему, активному пользователю, выполнившему вход в систему.
HKEY_LOCAL_MACHINE (HKLM)	Раздел содержит настройки, относящиеся к вашему компьютеру и действительны для всех пользователей. Раздел содержит информацию об аппаратной конфигурации и установленном программном обеспечении.
HKEY_USERS (HKU)	Этот раздел содержит настройки для всех пользователей компьютера
HKEY_CURRENT_CONFIG (HKCC)	Это ссылка на HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Hardware Profiles\Current. Раздел

	содержит сведения о настройках оборудования, используемом локальным компьютером при запуске системы, т.е. содержит информацию о текущей конфигурации.

Вышеуказанные основные стандартные разделы вы не сможете удалить или переименовать. Некоторые разделы реестра являются энергозависимыми (volatile) и не хранятся в каком-либо файле. Операционная система создает и управляет этими разделами полностью в памяти, поэтому они являются временными по своей природе. Система создает энергозависимые разделы каждый раз при начальной загрузке. Например, HKEY_LOCAL_MACHINE\HARDWARE − раздел реестра, который хранит информацию по физическим устройствам и назначенным им ресурсам. Назначение ресурса и аппаратное обнаружение происходят каждый раз при загрузке системы, поэтому логично, что эти данные не записываются на диск.

Раздел HKEY_USERS содержит все активные загруженные параметры пользователя. Он имеет не менее трёх ключей:

- Подраздел DEFAULT, где хранится используемая конфигурация, когда ни один из пользователей ещё не вошёл в компьютер. То есть ещё видим приглашение на вход в систему.
- Дополнительный подраздел, который имеет имя в соответствии с security ID текущего пользователя (SID). Этот подключ реестра содержит конфигурацию текущего пользователя. Если пользователь вошёл удалённо, данные для конфигурации пользователя сохраняются в системном реестре местного компьютера. Данные из HKEY_USERS\%SID% также появляются в HKEY_CURRENT_USER.
- Дополнительный подраздел, который имеет имя в соответствии с SID текущего пользователя с суффиксом Classes. Этот раздел

содержит классы текущего пользователя. Данные в HKEY_USERS\%SID%_Classes также содержатся в HKEY_CLASSES_ROOT.

Файлы реестра Windows:

Имя файла	**Соответствующий куст реестра Windows**
SAM	HKEY_LOCAL_MACHINE\SAM
SECURITY	HKEY_LOCAL_MACHINE\Security
Software	HKEY_LOCAL_MACHINE\Software
System	HKEY_LOCAL_MACHINE\System HKEY_CURRENT_CONFIG
Default	HKEY_USERS\.DEFAULT
Файлы Ntuser.dat	HKEY_CURRENT_USER (эти файлы хранятся в C:\Documents and Settings\%UserName%) Содержат конфигурацию для конкретного пользователя.

По умолчанию почти все файлы кустов: Default, SAM, Security, Software и System, сохраняются в папке %SystemRoot%\System32\Config.

Папка %SystemRoot%\Profiles содержит настройки для каждого пользователя компьютера.

Если есть сомнения, то точный список файлов реестра Windows можно посмотреть здесь: HKEY_LOCAL_MACHINE\System\CotnrolSet\Control\HiveList\ при начальной загрузке к этому разделу обращается Configuration Manager, чтобы проинициализировать все основные разделы реестра.

В операционной системе Windows сведения о конфигурации системы централизованно размещены в реестре. Это упрощает администрирование компьютера или сети, но, вместе с тем, одно неправильное изменение в реестре может вывести операционную систему из строя.

Перед внесением изменений в реестр делайте резервную копию.

Не заменяйте реестр вашей операционной системы реестром другой версии операционных систем Windows или Windows NT.

Для редактирования реестра используйте редактор реестра или другие программы, которые обеспечивают безопасные методы работы с реестром.

Основная часть

1) Какие конкретно ветки и ключи доступны пользователю хотя бы на чтение; только Администратору; только System. (Перечислить их названия.)

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

3) Описать в отчете способы восстановления реестра. (**Для нечетных вариантов.**) (В отчете: подробное описание выполнения задания со скриншотами.)

4) Данное задание выполняется исходя из варианта. Необходимо указать 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 3е суток до сдачи данной лабораторной работы*.)

Варианты заданий (вариант необходимо получить у преподавателя):

1. вариант:
    a. Переход дисплея в экономичный режим ожидания.
    b. Отключение запроса пароля при выходе из ждущего режима.
    c. Отключение сообщение об ошибках на странице и их отладку в Internet Explorer.

2. вариант:
    a. Настройка службы Superfetch: включение механизма Prefetcher.
    b. Отключение всплывающей подсказки для элементов рабочего стола.
    c. Блокировка кнопок «Вперед» и «Назад» в Internet Explorer.
3. вариант:
    a. Настройка службы Superfetch: включение механизма Prefetcher только для загрузки системы.
    b. Увеличение скорости выключения компьютера.
    c. Скрытие закладки «Рабочий стол» в свойствах экрана.
4. вариант:
    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.
5. вариант:
    a. Настройка службы Superfetch: отключение трассировки службы.
    b. Изменение заставки.
    c. Ускорение открытия меню «Пуск».
6. вариант:
    a. Вид панели управления, задать классический.
    b. Скрытие пароля к сетевым ресурсам, поставить «не скрывать».
    c. Автоматическое завершение всех приложений при выключении компьютера.
7. вариант:
    a. Настройка службы Superfetch: включение службы Superfetch.
    b. Отключение истории списка последних документов.
    c. Отключение вызова диспетчера задач.

8. вариант:
    a. Настройка службы Superfetch: включение службы Superfetch только для загрузки системы.
    b. Отключение выделения недавно установленных программ.
    c. Изменение задержки предварительного просмотра панели задач.
9. вариант:
    a. Настройка службы Superfetch: включение службы Superfetch во время работы, но при этом чтобы была отключена при загрузки системы.
    b. Сортировка меню по алфавиту.
    c. Установка версии Windows на рабочем столе.
10. вариант:
    a. Включение доступа к настройкам DVD в Windows Media Player.
    b. Отключение добавления приставки "Ярлык для" к названию ярлыков при их создании.
    c. Включение автоматического открытия папок после загрузки системы, если они не были закрыты пользователем перед перезагрузкой.
11. вариант:
    a. Настройка службы Superfetch: включение службы Superfetch во время работы, и при загрузки системы.
    b. Удаление пункта «Справка».
    c. Удаление пункта «Выход из системы»
12. вариант:
    a. Отключение кэширования изображений.
    b. Отключение автозапуска CD/DVD-дисков.
    c. Не выгрузка из оперативной памяти коды ядра и драйверов.

13.вариант:

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

14.вариант:

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

15.вариант:

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.

16. вариант:

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.

17.вариант:

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

18.вариант:

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

19.вариант:

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

20.вариант:

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.

21.вариант:

a. Отображение значков в меню «Пуск» крупными.
b. Требование пароля только из букв и цифр.
c. Отмену сохранения информации о действиях пользователя.

22.вариант:

a. Скрытие/отображение пользователей в диалоговом окне входа в систему.
b. Изменение серийного номера Windows.
c. Отключение отправки отчетов об ошибках в MS Office.

23.вариант:

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

24.вариант:

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

25.вариант:

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.

26.вариант:

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 вызов диспетчера задач.

27.вариант:

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

28.вариант:

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

29.вариант:

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

30.вариант:

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.

31. вариант:

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.

32.вариант:

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

33.вариант:

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

34.вариант:

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

35.вариант:

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.

36.вариант:

a. Отображение значков в меню «Пуск» крупными.
b. Требование пароля только из букв и цифр.
c. Отмена сохранения информации о действиях пользователя.

37.вариант:

a. Скрытие/отображение пользователей в диалоговом окне входа в систему.
b. Изменение серийного номера Windows.
c. Отключение отправки отчетов об ошибках в MS Office.

38.вариант:

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

39.вариант:

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

40.вариант:

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.

41.вариант:

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 вызов диспетчера задач.

42.вариант:

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

43.вариант:

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

44.вариант:

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

45. вариант:

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

46.вариант:

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

47.вариант:

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

48.вариант:

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.

49.вариант:

a. Настройка службы Superfetch: включение механизма Prefetcher только для загрузки системы.
b. Увеличение скорости выключения компьютера.
c. Скрытие закладки «Рабочий стол» в свойствах экрана

50.вариант:

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

51.вариант:

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

52.вариант:

a. Вид панели управления, задать классический.
b. Скрытие пароля к сетевым ресурсам, поставить «не скрывать».
c. Автоматическое завершение всех приложений при выключении компьютера.

53.вариант:

a. Настройка службы Superfetch: включение службы Superfetch.
b. Отключение истории списка последних документов.
c. Отключение вызова диспетчера задач.

54.вариант:

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

55.вариант:

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

5) Настроить на аудит какую-либо ветку реестра и отобразить настройку отчет по событиям для данной ветки в отчете (минимум 5 подразделов). (В отчете: подробное описание выполнения задания со скриншотами.)

6) Получить права доступа на редактирование к разделам SAM и Security для созданного вами Администратора. (В отчете: подробное описание выполнения задания со скриншотами.)

Дополнительная часть

1) Написать скрипт, который будет менять заголовок в браузере Internet Explorer. (В отчете: скриншоты браузера и скрипт.)

2) При помощи Process Monitor для какой-либо программы (notepad, wordpad, или др. текстовый редактор) установить адрес хранения настроек (размер шрифта, имя шрифта и т.п.) в реестре. Попробовать поменять настройки через реестр вручную, проследить и отобразить в отчете реакцию программы. (В отчете: подробное описание выполнения задания со скриншотами.)

3) Написать программу аналог Regedit. Должна быть реализована возможность просмотра всех параметров, их редактирование. (В отчете: исходный код и интерфейсы.)

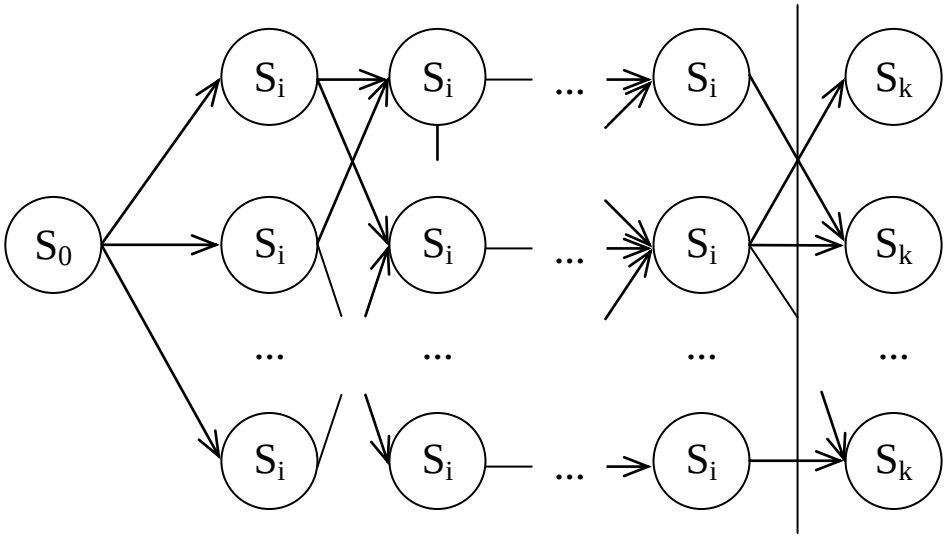
Лабораторная работа №4

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 спец. 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;
- XSS (межсайтовый скриптинг) ;
- SQL-Injection;
- Mail-bombing;
- DNS Cache Poisoning (Атака Каминского) ;
- Padding Oracle;
- XSRF;
- переполнение буфера;
- MITM;
- 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. Возможно 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. Белозубов А.В., Билевич С.А., Николаев Д.Г. 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

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра была создана в 1937 году и является одной из старейших и авторитетнейших научно-педагогических школ России. Первым заведующим кафедры был профессор М.Ф. Маликов.

Первоначально кафедра называлась кафедрой Счетно-математических приборов и занималась разработкой электромеханических вычислительных устройств и приборов управления. На кафедре развивалось два направления вычислительной техники: машины непрерывного действия (приборы управления) и машины дискретного действия (счетные или, как они тогда назывались, счетно-аналитические).

В сентябре 1937 года при кафедре была создана лаборатория. Ее первым заведующим был К.Г.Кроль (впоследствии - доцент кафедры). К осени 1939 года кафедра стала одной из ведущих в институте. Для чтения отдельных разделов курсов и руководства дипломными проектами привлекались ведущие специалисты промышленности.

С 1944 года кафедрой заведовал профессор С.А. Изенбек. В послевоенный период на кафедре были развернуты исследования принципов построения электромеханических вычислительных устройств. На их основе были разработаны тренажеры, приборы для автоматизации прочностных расчетов и обработки результатов ходовых испытаний кораблей.

В 1950-х годах на кафедре функционировали три учебно-исследовательские лаборатории: электромеханических и счетно-решающих устройств, счетных и счетно-аналитических машин, приборов управления. В них исследовались счетно-решающие устройства на потенциометрах, приборы для автоматизации расчетов и электронные счетные устройства.

Эксперименты по применению электронных машин для выполнения операций над числами, проводимые доцентом Ф.Я. Галкиным и инженером М.Н. Романовым, позволили разработать проект электронной вычислительной машины для инженерных расчетов. Он был поддержан руководителем проблемной оптической лаборатории института профессором М.М. Русиновым.

В 1956 году началось изготовление ЭВМ. Создание электронно-вычислительных машин собственной разработки началось в ЛИТМО, когда ЭВМ, такие как «Урал», еще только создавались. В 1962-1964 годах была создана ЭВМ «ЛИТМО-2» на ферриттранзисторных модулях.
В 1962 году заведующим кафедрой был избран профессор С.А. Майоров.
С начала 60-х годов на кафедре развернулись работы по методам проектирования ЭВМ: иммитационному моделированию цифровых устройств (Новиков Г.И.), анализу и синтезу переключательных схем (Немолочнов О.Ф.), тестированию и диагностике схем (Гольдман Р.С., Немолочнов О.Ф.), машинному анализу электронных схем (Ермолаенков Э.Г.), монтажно-коммутационному проектированию (Шипилов П.А.). Автоматизация проектирования ЭВМ стала основным научным направление кафедры.
В 1963 году кафедра была переименована в кафедру Вычислительной техники.
Кафедра Вычислительной техники является одной из крупнейших в Университете, на которой работают высококвалифицированные специалисты, в том числе 8 профессоров и 15 доцентов, обучающие около 500 студентов и 30 аспирантов.
На кафедре ВТ проводятся научные исследования в соответствии с программой развития научной школы кафедры «Организация вычислительных систем и сетей», включенной в реестр ведущих научных и научно-педагогических школ Санкт-Петербурга. Магистранты и аспиранты активно участвуют в научно-исследовательских работах по следующим основным направлениям.
Сотрудники кафедры участвуют в работе Международных научных лабораторий:

- «Архитектура и методы проектирования встраиваемых систем и систем на кристалле»;
- «Лаборатория нелинейных и адаптивных систем управления»;
- «Многомодальные биометрические и речевые системы».

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 100
Отпечатано на ризографе

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