# Виды угроз

1. Естественные (ураган ебучий)
2. Искусственные
   1. Непреднамеренные (несовместимая прога = потеря информации)
   2. Преднамеренные извне или изнутри организации
      1. Нежелательный контент
      2. Несанкционированный доступ
      3. Утечки данных
      4. Потеря данных
      5. Мошенничество
      6. Кибервойны
      7. Кибертерроризм

# Управление изменениями требований

1. Оформить официальный запрос на изменение
2. Проанализировать запрос
   * Разработать стратегию реализации
   * Рассчитать стоимость реализации
   * Проанализировать все последствия для безопасности
3. Зарегистрировать запрос на изменение
4. Передать запрос на изменение для утверждения
5. Разработать изменение
   * Переписать код продукта, добавить или исключить требуемую изменением функциональность
   * Связать эти изменения в коде с официальным запросом на изменение
   * Передать программное обеспечение для тестирования и подтверждения качества
   * Повторять, пока не будет обеспечено надлежащее качество
   * Произвести изменения версии
6. Отчитаться о результатах

# Из работы 1

## 1. диспетчер учетных записей (SAM - Security Account Manager)

файл в системах Windows (XP, Vista, 7, 8.1, 10), в котором хранятся пароли пользователей. Используется при аутентификации пользователей. Пароли хранятся хешированные. Находится в реестра HKLM/SAM

## 2. монитор безопасности (SRM - Security Reference Monitor)

в системах Windows система, определяющая для пользователя наличие доступа к ресурсам.

## 3. маркер доступа (access token)

программный объект в системах Windows, идентифицирующий контекст безопасности процесса или потока. В нем хранится информация о привилегиях пользователя или группы пользователей.

## 4. идентификатор безопасности (SID - Security Identifier)

уникальный и неизменяемый идентификатор пользователя или группы пользователей в системах Windows.

## 5. привилегии пользователя

это права пользователя на выполнение определнных действий

## 6. права пользователя (user rights)

бля честно хз чем отличвается от привилегий

## 7. объект доступа

часть информационной системы, доступ к которой может быть ограничен политикой безопасности.

## 8. субъект доступа

это лицо или процесс, действия которого регламентируются правилами разграничения доступа.

## 9. олицетворение (impersonation)

акт выдачи лицом А самого себя за лицо Б.

## 10. список контроля доступа (ACL - Access Control List)

это список записей, связанных с определенным объектом, которые определяют какие пользователи имеют доступ и какие операции им доступны

## 11. учетная запись

<https://dic.academic.ru/dic.nsf/ruwiki/92937> Учётная запись — запись, содержащая сведения, которые пользователь сообщает о себе некоторой компьютерной системе. Содержит информацию необходимую для идентификации пользователя наряду с дополнительной инфой (пол, раса, размер хуя и тп)

## 12. домен

<https://en.wikipedia.org/wiki/Windows_domain> A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database located on one or more clusters of central computers known as domain controllers.

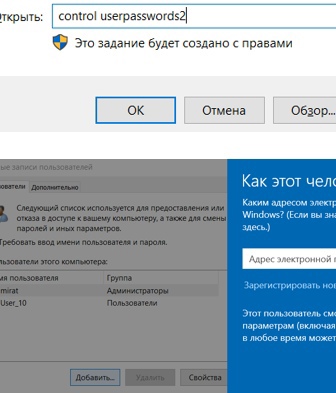
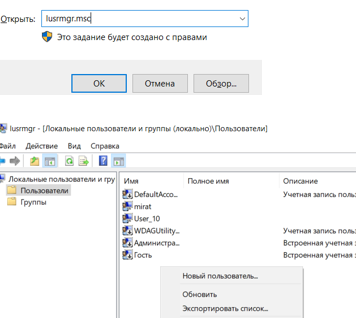
# Работа 1

## Перечислите типы учетных записей.

Администратор, пользователь и гость (нет в 10ке)

## Перечислите способы создания учетных записей.

<https://ichip.ru/sovety/5-sposobov-dobavit-novuyu-uchetnuyu-zapis-v-windows-10-229222>

1. Через параметры системы
2. Через утилиту “Учетные записи пользователей”  
   
3. Через групповые политики  
   
4. Cmd  
   

## Что понимается под идентификацией пользователя?

<https://www.aladdin-rd.ru/company/pressroom/articles/obzor_tehnologij_identifikacii_i_autentifikacii>

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.

## Что понимается под аутентификацией пользователей?

<https://www.aladdin-rd.ru/company/pressroom/articles/obzor_tehnologij_identifikacii_i_autentifikacii> Аутентификация - процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор. В большинстве случаев она состоит в процедуре обмена между входящим в систему объектом и ресурсом, отвечающим за принятие решения ("да" или "нет"). Таким образом, идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности пользователей.

## Перечислите возможные идентификаторы при реализации механизма идентификации.

<https://ru.wikipedia.org/wiki/%D0%98%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B>)

* Логин
* Имя файла
* Я хуй его знает

## Перечислите возможные идентификаторы при реализации механизма аутентификации.

<https://dic.academic.ru/dic.nsf/ruwiki/92937>

1. Пароль
2. Биометрия
3. Секретные вопросы
4. Я хуйего знает

<https://www.aladdin-rd.ru/company/pressroom/articles/obzor_tehnologij_identifikacii_i_autentifikacii>

* Штрих-код
* Радиочастотная (лол)
* Биометрия
* Карты с магнитной полос кой

<https://intuit.ru/studies/courses/10/10/lecture/314>

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

1. нечто, что он знает (пароль, личный *идентификационный* номер, *криптографический ключ* и т.п.);
2. нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
3. нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

## Какой из механизмов (аутентификация или идентификация) более надежный? Почему?

Аутентификация офк. Можно заявить что являешься одменом (мой логин - cooladmin) но без пароля не пустит

## Опишите механизм аутентификации пользователя.

<https://www.aladdin-rd.ru/company/pressroom/articles/obzor_tehnologij_identifikacii_i_autentifikacii>

Своими словами:

* Получил идентификатор
* Спрашиваешь пароль
* Или одноразовый праоль
* Цифровой сертификат (хз, лучше не говори тупа)
* Смарт-карта, usb-ключ

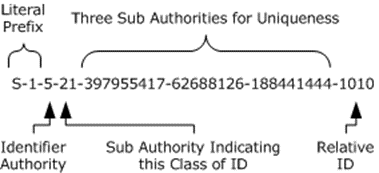
После того как субъект безопасности вводит с клавиатуры или иным способом предоставляет необходимую для идентификации информацию (например, имя пользователя, маркер безопасности), он должен ввести с клавиатуры или представить частную информацию для аутентификации (например, пароль и PIN-код). В Windows субъект безопасности вводит эту информацию на экране регистрации с помощью программ Microsoft Graphical Identification and Authentication DLL (msgina.dll) и Winlogon.exe. Протокол аутентификации и механизм системы кодируют представленную информацию на настольном компьютере и передают запрос аутентификации

## Структура маркера доступа.

<https://en.wikipedia.org/wiki/Access_token>

1. Идентификатор (видимо, самого маркерыча)
2. Идентификатор связанный с сессией логина (logon session)
3. Идентификатор юзера
4. Идентификатор группы (бля заебали идентификатор идентификатор)
5. Идентификатор (лол) группы разграничения прав (необязательно)
6. Привилегии
7. Дефолтный владелец, главная группа и ACL (acess control list, См выше) токен

## Структура SID.



* S - префикс (всегда такой лол)
* 1 - номер ревизии (всегда такая лол)
* 5 - идентификатор источника, который выдал (всегда вроде тоже. Вроде 5 это винда)
* 21 - … сначала домен идет (21), потом вроде ид внутри домена
* Относительный идентификатор (для всех юзер или групп созданных не по дефолту значение будет 1000+)

# Работа 2

## Что такое файловая система?

<https://www.sites.google.com/a/i-dist.ru/informacionnye-tehnologii-ucebnoe-posobie/operacionnye-sistemy-personalnogo-komputera/fajly-i-fajlovaa-sistema>

Файловая система - это система хранения файлов и организации каталогов.

Файл - это определенное количество информации (программа или данные), имеющее имя и хранящееся в долговременной (внешней) памяти.

<https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0>

Файловая система определяет формат содержимого и способ физического хранения информации, которую принято группировать в виде файлов. Конкретная файловая система определяет размер имен файлов (и каталогов), максимальный возможный размер файла и раздела, набор атрибутов файла. Некоторые файловые системы предоставляют сервисные возможности, например, разграничение доступа или шифрование файлов.

## Перечислите существующие файловые системы

Ntfs (windows)

Fat32, exfat (windows, флешки, microsd)

Nas (хз)

Ext4 (android + unix)

Hfs+, hfsx, apfs, wtfs (apple)

## Какова модель разграничения доступа в ОС Windows?

В наиболее распространенных сегодня ОС Windows и UNIX используется дискреционное разграничение доступа.

Дискреционная модель разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретных пользователей или групп. Ее недостатком является отсутствие механизмов слежения за безопасностью потоков информации. Это означает, что права на доступ к объекту проверяются только при первом обращении к объекту. При этом возникает опасность переноса информации из защищенного объекта в общедоступный.

<https://intuit.ru/studies/professional_retraining/962/courses/217/lecture/5609?pag>

Известно, что одним из важнейших компонентов системы безопасности ОС Windows является система контроля и управления дискреционным доступом. Для ее описания принято использовать формальные модели. Хотя применение формальных моделей защищенности не позволяет строго обосновать безопасность информационных систем (ИС) для ряда наиболее интересных случаев, они формируют полезный понятийный аппарат, который может быть применен для декомпозиции и анализа исследуемой системы.

Для построения формальных моделей безопасности принято представлять ИС в виде совокупности взаимодействующих сущностей - субъектов (s) и объектов (o).

Защищаемые объекты Windows включают: файлы, устройства, каналы, события, мьютексы, семафоры, разделы общей памяти, разделы реестра ряд других. Сущность, от которой нужно защищать объекты, называется "субъектом". Субъектами в Windows являются процессы и потоки, запускаемые конкретными пользователями. Субъект безопасности - активная системная составляющая, а объект - пассивная.

Помимо дискреционного доступа Windows поддерживает управление привилегированным доступом. Это означает, что в системе имеется пользователь-администратор с неограниченными правами. Кроме того, для упрощения администрирования (а также для соответствия стандарту POSIX) пользователи Windows объединены в группы. Принадлежность к группе связана с определенными привилегиями, например, привилегия выключать компьютер. Пользователь, как член группы, облекается, таким образом, набором полномочий, необходимых для его деятельности, и играет определенную роль. Подобная стратегия называется управление ролевым доступом.

## Что такое DACL?

Discretionary Access Control List (DACL) — дискретный (избирательный) список контроля доступа. Именно этот список формирует разрешения файловой системы, с помощью которых происходит управление доступом к объекту..

## Перечислите существующие разрешения для пользователей.

<https://windowsnotes.ru/other/nastrojka-razreshenij-fajlovoj-sistemy-ntfs/>

Базовые:

1. List Folder Contents (Просмотр содержимого директории) — позволяет зайти в папку и просмотреть ее содержимое;
2. Read  (Чтение) — дает право на открытие файла\папки на чтение, без возможности изменения;
3. Read & execute (Чтение и выполнение) — позволяет открывать файлы на чтение, а также запускать исполняемые файлы;
4. Write (Запись) — разрешает создавать файлы\папки и редактировать файлы, без возможности удаления;
5. Modify (Изменение) — включает в себя все вышеперечисленные разрешения. Имея разрешение Modify можно создавать, редактировать и удалять любые объекты файловой системы;
6. Full Control (Полный доступ) — включает в себя разрешение Modify, кроме того позволяет изменять текущие разрешения объекта.

Дополнительные:

1. Траверс папок / Выполнение файлов
2. Содержимое папки / чтение данных
3. Чтение расширенных атрибутов
4. Создание файлов / запись данных
5. Создание папок / добавление данных
6. Запись атрибутов
7. Запись расширенных атрибутов
8. Удаление подпапок и файлов
9. Удаление
10. Чтение разрешений
11. Изменение разрешений
12. Смена владельца

## Расскажите про наследование разрешений.

Если вы установили определенные разрешения для папки, то эти разреше­ния распространяются на все ее файлы и подпапки (хотя обычно во время настройки Windows спрашивает, нужно ли включить наследование). Когда разрешения для родительской папки распространяются также и на дочернюю папку или файл, то говорят, что дочерний объект «наследует» разрешения от родительского. Изменить унаследованные разрешения дочернего объекта невозможно, по крайней мере, пока включено наследование от предка.

## Перечислите способы для разграничения доступа.

Существуют следующие методы разграничения доступа:

* разграничение по спискам;

При разграничении доступа по спискам задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

* использование матрицы установления полномочий;

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в ИС, а столбцами — объекты (ресурсы) ИС. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.



* разграничение по уровням секретности и категориям;

При разграничении по степени секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень конфиденциальности не выше, чем ему определен. Например, пользователь имеющий доступ к данным «секретно», также имеет доступ к данным «конфиденциально» и «общий доступ».

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы ИС разделяются по уровням важности, причем определенному уровню соответствует категория пользователей.

* парольное разграничение.

Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

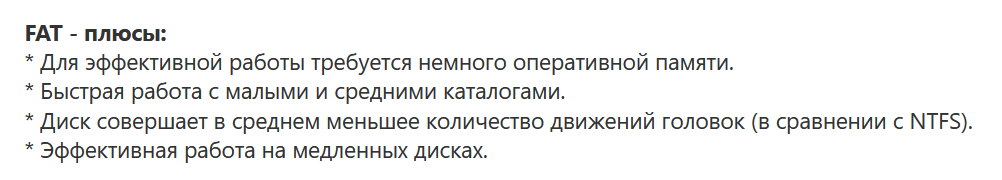
## В чем отличие между пользовательскими и системными переменными окружения

Очень похоже на то, как работает реестр в Windows, у нас есть переменные среды системы и пользователя. Системные переменные являются общесистемными и не меняются от пользователя к пользователю. Принимая во внимание, что пользовательские среды настраиваются по-разному от пользователя к пользователю. Вы можете добавить свои переменные под пользователем, чтобы другие пользователи не влияли на них.

**Системные переменные** имеют меньший приоритет, чем **пользовательские переменные**. Таким образом, если есть некоторые пользовательские переменные с тем же именем, что и системные переменные, то будут учитываться пользовательские переменные. Переменная пути генерируется другим способом. Эффективным путем будет переменная «Пользовательский путь», добавляемая к переменной «Системный путь». Таким образом, порядок записей будет системных записей, за которыми следуют пользовательские записи.

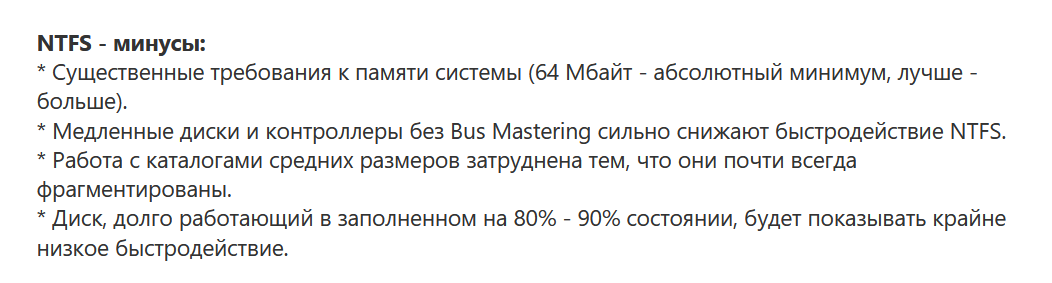
## Перечислите три достоинства FAT.

<http://2828.ru/pro/fat32_vs_ntfs>



## Перечислите три недостатка NTFS.

<http://2828.ru/pro/fat32_vs_ntfs>



# Работа 3

## Что такое реестр?

Реестр Windows (англ. Windows Registry), или системный реестр — иерархически построенная база данных параметров и настроек в большинстве операционных систем Microsoft Windows.

Реестр содержит информацию и настройки для аппаратного обеспечения, программного обеспечения, профилей пользователей, предустановки. Большинство изменений в Панели управления, ассоциации файлов, системные политики, список установленного ПО фиксируются в реестре.

Реестр Windows был введён для упорядочения информации, хранившейся до этого во множестве INI-файлов, обеспечения единого механизма (API) записи-чтения настроек и избавления от проблем коротких имён, отсутствия разграничения прав доступа и медленного доступа к ini-файлам, хранящимся на файловой системе FAT16, имевшей серьёзные проблемы быстродействия при поиске файлов в каталогах с большим их количеством. Со временем (окончательно — с появлением файловой системы NTFS) проблемы, решавшиеся реестром, исчезли, но реестр остался из-за обратной совместимости и присутствует во всех версиях Windows, включая последнюю. Поскольку сейчас не существует реальных предпосылок для использования подобного механизма, Microsoft Windows — единственная (не считая ReactOS и eComStation) операционная система из используемых сегодня, в которой используется механизм реестра операционной системы.

## Как запустить редактор реестра?

Существует два способа открыть редактор реестра в Windows 10:

1. В поле поиска на панели задач введите regedit, а затем выберите Редактор реестра (настольное приложение) в результатах.
2. Щелкните правой кнопкой мыши кнопку Начните и выберите выполнить. Введите regedit в поле “Открыть”: и выберите ОК.

## Как сохранить реестр перед редактированием?

1. Открыть редактор реестра
2. Выберите в открывшемся Редакторе реестра меню Файл / Экспорт.
3. Укажите путь для сохранения файла резервной копии реестра с расширением .reg и нажмите Сохранить.

## Как восстановить реестр?

Способ 1

* Открыть редактор реестра
* Выберите в открывшемся **Редакторе реестра** меню **Файл** / **Импорт**.
* Укажите путь для к сохранённому раннее файлу резервной копии реестра с расширением **.reg** и нажмите **Открыть**.
* Перезагрузите компьютер для завершения процесса восстановления резервной копии реестра

Способ 2

* Кликните дважды на .reg-файле реестра (файл сохранённой раннее резервной копии реестра).
* Подтвердите необходимость редактирования реестра.
* Перезагрузите компьютер.

Способ 3

* Кликните правой кнопкой мыши на файле резервной копии реестра.
* Выберите пункт Слияние.
* Перезагрузите компьютер.

Также возможен вариант использования восстановления системы, так как точка восстановления хранит в себе параметры реестра. Таким образом, нужно лишь откатиться к созданной точке восстановления либо импортировать значение файла точки восстановления используя диск восстановления и командную строку, запущенную из оного средства.

## Расскажите о структуре реестра.

Редактор реестра очень похож на проводник, а структура реестра похожа на файловую систему вашего компьютера:

* слева отображаются разделы, похожие на папки, внутри них есть подразделы (совсем как подпапки);
* справа отображаются параметры (очень похожи на файлы) и их значения.

Реестр Windows 10, 8, 7, XP состоит из пяти стандартных разделов – корневых ключей:

* **HKEY\_CLASSES\_ROOT** – информация о зарегистрированных в Windows типах файлов
* **HKEY\_CURRENT\_USER** – настройки пользователя, вошедшего в Windows
* **HKEY\_LOCAL\_MACHINE** – настройки, относящиеся к компьютеру
* **HKEY\_USERS** – настройки для всех пользователей
* **HKEY\_CURRENT\_CONFIG** – сведения о настройках оборудования

Для простоты, их часто указывают в сокращенном обозначении (аббревиатура из первых букв): **HKCR, HKCU, HKLM, HKU, HKCC**.

Параметры реестра делятся на три основных типа (и несколько разновидностей):

* **Строковые параметры –** REG\_SZ
* **Двоичные параметры –** REG\_BINARY
* **DWORD-параметры –** REG\_DWORD

## Из каких файлов состоит реестр? Где они расположены?

Файлы, составляющие реестр, хранятся в папке %systemroot%/system32/config и состоят из:

1. SAM - HKEY\_LOCAL\_MACHINE\SAM
2. SECURITY - HKEY\_LOCAL\_MACHINE\Security
3. software - HKEY\_LOCAL\_MACHINE\Software
4. system - HKEY\_LOCAL\_MACHINE\System & HKEY\_CURRENT\_CONFIG
5. default - HKEY\_USERS\.DEFAULT
6. Ntuser.dat - HKEY\_CURRENT\_USER (этот файл хранится в %SystemRoot%\Profiles\%username%)

Также имеются файлы с другими расширениями:

* .alt - Содержит резервную копию раздела HKEY\_LOCAL\_MACHINE\System. Только у System есть .alt файлы.
* .log - Файл регистрации изменений значений параметров в разделе.
* .sav - Копия раздела, создаваемая в конце text mode stage установки.

## Расскажите о назначении реестра.

Реестр – это база данных (БД), предназначенная для хранения сведений о конфигурации компьютера. Реестр содержит сведения к которым Windows постоянно обращается во время работы:

1. Профили всех пользователей;
2. Данные об установленных программах и типов документов, создаваемых каждой программой;
3. Значения свойств для папок и значков программ;
4. Конфигурация оборудования, установленного в операционной системе;
5. Данные об используемых портах.

## Назовите ключи, имеющие псевдонимы.

Для простоты, их часто указывают в сокращенном обозначении (аббревиатура из первых букв): **HKCR, HKCU, HKLM, HKU, HKCC**.

## Расскажите о способах редактирования реестра.

Основные операции, которые можно выполнить в Редакторе реестра, это:

* **Поиск** раздела реестра, строк или параметра.
* **Добавление** раздела или параметра реестра. В левой части редактора реестра выделите раздел, в который необходимо добавить подраздел. В меню “Правка” выберите команду “Создать” – “Раздел” – введите имя нового раздела и нажмите Enter.  
  Для создания нового параметра выберите в меню “Правка” один из типов параметров: Строковый, Двоичный, Параметр DWORD, Мультистроковый, либо Расширяемый строковый параметр. Затем введите имя параметра и нажмите Enter.
* **Удаление** раздела или параметра. Выделите удаляемый раздел или параметр – в меню “Правка” выберите “Удалить” (либо нажмите на клавиатуре Delete)
* **Изменения значения** параметра. Выделите параметр, значение которого требуется изменить. В меню “Правка” выберите команду “Изменить”. В поле “Значение” введите новое значение параметра и нажмите кнопку “ОК”.
* **Переименование** раздела или параметра реестра. Выберите раздел или параметр, который требуется переименовать. В меню “Правка” выберите команду “Переименовать”. Введите новое имя и нажмите клавишу Enter.

## Назовите основные разделы и их назначение

|  |  |
| --- | --- |
| Раздел реестра | Описание |
| HKEY\_CLASSES\_ROOT (HKCR) | Раздел хранит информацию о всех типах файлов, о которых должна знать Windows (avi, doc, jpg и все остальные). Для каждого типа указана программа, связанная с ним, закреплен значок, который отображается в проводнике, приведены команды, которые можно использовать для данных файлов (открыть, печать и т.д.) После установки различных программ, здесь регистрируются новые типы файлов (например, после установки архиватора 7-Zip появляется тип файла .7z) Раздел является копией подраздела HKEY\_LOCAL\_MACHINE\Software\Classes |
| HKEY\_CURRENT\_USER (HKCU) | Этот раздел содержит настройки пользователя, вошедшего в систему в данный момент. Здесь хранятся настройки экрана, раскладка клавиатуры, сетевые подключения, настройки программ и многое другое. Большинство рекомендаций по настройке реестра относятся к этому разделу. |
| HKEY\_USERS (HKU) | Здесь находятся настройки всех пользователей операционной системы, а также настройки по умолчанию. На самом деле раздел HKEY\_CURRENT\_USER – это один из подразделов раздела HKEY\_USERS и все изменения настроек, совершенные пользователем, сохраняются в выделенном для него подразделе. |
| HKEY\_LOCAL\_MACHINE (HKLM) | В этом разделе хранится информация о настройках компьютера (программной и аппаратной конфигурации). Всё, что вы измените в этом разделе, будет влиять на всех пользователей ПК. Этот раздел второй по популярности вносимых изменений. |
| HKEY\_CURRENT\_CONFIG (HKCC) | Раздел содержит информацию о настройке оборудования для текущего сеанса (профиль оборудования). Этот раздел является копией подраздела «HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles» и практически не используется при ручных изменениях. |