Лабораторная работа № 1

Тема: Защита файловой системы

Цель работы:

1. Изучить и приобрести навыки установления разрешений на доступ к файлам и папкам.
2. Изучить и приобрести навыки шифрования файлов и папок
3. Изучить и приобрести навыки шифрования диска с помощью BitLocker

Учебные вопросы:

1. Установка разрешений на доступ к файлам и папкам
2. Шифрование файлов и папок
3. Шифрование диска с помощью BitLocker

Литература:

1. Конспект лекций
2. Мак Федрис, Пол. М Microsoft Windows. Полное руководство: Пер с англ. – М.: ООО «И.Д. Вильямс», 2010. – 800 с.: ил. – Парал. тит. англ.

Учебно-материальное обеспечение:

1. Сегмент локальной вычислительной сети кафедры.
2. Рабочие станции (персональные компьютеры).
3. ОС Microsoft Windows.

Учебный вопрос 1. Учётные записи и права

Учётная запись - хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Учётная запись, как правило, содержит сведения, необходимые для опознания пользователя при подключении к системе, сведения для авторизации и учёта. Это идентификатор пользователя (**login**) и его пароль. Пароль или его аналог, как правило, хранится в **зашифрованном или хэшированном** виде для обеспечения его безопасности. Для аутентификации могут также использоваться специальные файлы-ключи (которые можно сохранять на разных носителях информации) либо аппаратные средства (вырабатывающие одноразовые ключи, считывающие биометрические характеристики и т.п.), а также одноразовые пароли.

Для повышения надёжности, наряду с ключом или паролем могут быть предусмотрены иные средства сверки - например, особый потайной вопрос (или несколько вопросов) такого содержания, что ответ может быть известен только пользователю. Такие вопросы и ответы также хранятся в учётной записи.

Учётная запись может содержать также дополнительные опросные данные о пользователе - имя, фамилию, отчество, псевдоним, пол, народность, расовую принадлежность, вероисповедание, группу крови, резус-фактор, возраст, дату рождения, адрес e-mail, домашний адрес, рабочий адрес, нетмейловый адрес, номер домашнего телефона, номер рабочего телефона, номер сотового телефона, номер ICQ, идентификатор Skype, ник в IRC, другие контактные данные систем мгновенного обмена сообщениями, адрес домашней страницы и/или блога в паутине или Интранете, сведения об увлечениях, о круге интересов, о семье, о перенесённых болезнях, о политических предпочтениях, о партийной принадлежности, о культурных предпочтениях, об умении общаться на иностранных языках и т.п.. Конкретные категории данных, которые могут быть внесены в такой опросник, определяются создателями и (или) администраторами системы. Учётная запись может также содержать одну или несколько фотографий или аватар пользователя. Учётная запись пользователя также может учитывать различные статистические свойства поведения пользователя в системе: давность последнего входа в систему, продолжительность последнего пребывания в системе, адрес использованного при подключении компьютера, частотность использования системы, общее и (или) удельное количество определённых действий, произведённых в системе, и так далее.

Учетная запись пользователя Windows представляет собой набор данных, определяющих, к каким папкам и файлам пользователь имеет доступ, какие изменения могут

вноситься пользователем в работу компьютера, а также персональные настройки пользователя, такие как фон рабочего стола и экранная заставка. Применение учётных записей позволяет нескольким пользователям работать на одном компьютере с использованием собственных файлов и параметров. Для доступа к учетной записи используется имя пользователя и пароль.

Существуют три типа учетных записей. Каждый тип дает пользователю разные возможности управления компьютером:

1) обычные учетные записи пользователей предназначены для повседневной работы;

2) учетные записи администратора предоставляют полный контроль над компьютером и применяются только в необходимых случаях;

3) учетные записи гостя предназначены для временного доступа к компьютеру.

Одной из главных отличительных особенностей профессиональных версий Windows воспринимается повышенное внимание к тому, кто и что делает на компьютере. Программа, которая исполняется на компьютере с установленной операционной системой Windows, *всегда запущена от имени какого-либо пользователя* и обладает данными ему правами. Если запущенная программа вызывает в свою очередь новую задачу, то она также будет выполняться в контексте вашего имени. Даже программы, являющиеся частью, операционной системы, например, служба, обеспечивающая печать на принтер, или сама программа, которая запрашивает имя и пароль у пользователя, желающего начать работу на компьютере, выполняются от имени определенной учетной записи **(Система).** И так же, как программы, запускаемые обычным пользователем, эти службы имеют права и ограничения, которые накладываются используемой учётной записью.

Операционная система «различает» пользователей не по их имени (полному или сокращённому сокращенному), а по специальному уникальному номеру (**идентификатору безопасности - SID**), который формируется в момент создания новой[1] учетной записи. Поэтому учетные записи можно легко переименовывать, менять любые иные их параметры. Для операционной системы после этих манипуляций ничего не измелится, поскольку такие операции не затрагивав идентификатор пользователя.

Примечание

При создании новой учетной записи обычно определяются только имя пользователя и его пароль. Но учетным записям пользователей - особенно при работе в компьютерных сетях - можно сопоставить большое количество, различных дополнительных параметров: сокращенное и полное имя, номера служебного и домашнего телефонов, адрес электронной почты и право удаленно подключения к системе и т. п. Такие параметры являются дополнительными, их определение и использование на практике зависит от особенностей построения конкретной компьютерной сети. Эти параметры могут быть использованы программным обеспечением, например, для поиска определенных групп пользователей (см., например, **группы по запросу).**

Стандартные учетные записи имеют идентичные SID[2]. Например, **S-1-5-18** - это SID учетной записи **Local System**; **S-l-5-19** - учетной записи **NT Authority\LocaI Service**; SID **S-1-5-20 «**принадлежит» учетной записи **NT Authority\Nerwork Service** и т. д. Учетные записи пользователя домена "построены" по такой же структуре, но обычно еще более "не читаемы". Вот пример реального доменного SID:

S-1-5-21-61356107-1110077972-1376457959-10462

Если при изменении имени входа пользователя в систему ничего "существенного" для системы не происходит - пользователь для нее не изменился, то операцию удаления учетной записи и последующего создания пользователя точно с таким же именем входа операционная система будет оценивать, как появление **нового** пользователя. Алгоритм формирования идентификатора безопасности пользователя таков, что практически исключается создание двух учётных записей с одинаковы номером. В результате новый

---

[1] Существуют многочисленные утилиты, которые позволяют, но имени входа пользователя определить его SID п наоборот. Например, такая утилита входит в состав **Resource Kit для Windows** (getsid). В статье **KB276208** базы знаний Microsoft приведен код на Visual Basic, который позволяет выполнить запросы SlD/имя в обычном сценарии. Код хорошо комментирован и легко может быть применен без поиска специализированных утилит. Можно также установить на компьютер утилиты Account Lockout and Management Tools (см. рис. 5.11), которые добавляют к оснастке управления пользователями в домене еще одну закладку свойств, на которой в том числе отображается имя пользователя.

[2] **Перечень Well Known Security Identifiers приведен, например, в KB243330.**

пользователь не сможет, получить доступ, например, к почтовому ящику, которым пользовался удалённый сотрудник с таким же именем, не прочитает зашифрованные им файлы и т.п.

При работе в компьютерной сети существуют два типа учетных записей.

1) **Локальные учетные записи** создаются на данном компьютере. Информация о них хранится локально (в локальной базе безопасности компьютера) и локально же выполняется аутентификация такой учетной записи (пользователя).

2) **Доменные учетные записи** создаются на контроллерах домена. И именно контроллеры домена проверяют параметры входа такого пользователя в систему.

Разные пользователи должны иметь разные права по отношению к компьютерной системе.

Если в организации всего несколько сотрудников, то администратору не представляет особого труда индивидуально распределить нужные разрешения и запреты. Хотя и в этом случае возникают проблемы, например, при переходе сотрудника на другую должность администратор должен вспомнить, какие права были даны ранее, "снять" их и назначить новые, но принципиальной необходимости использования каких-либо объединений, групп пользователей не возникает.

Иная ситуация в средней организации. Назначить права доступа к папке для нескольких десятков сотрудников - достаточно трудоемкая работа. В этом случае удобно распределять права не индивидуально, а по *группам пользователей*, в результате чего управление системой существенно облегчается.[3]

Исторически сложилось так, что существует ***несколько типов групп****. Связано это в основном с необходимостью совместимости различных версий операционных систем.*

Во-первых, есть группы, которым, как и пользователям, присваивается **идентификатор безопасности**. Это означает, что вы можете назначать *права доступа,* основываясь не на индивидуальном членстве, а сразу *всё группе пользователей*.

И есть **группы, которые не имеют такого SID**. Например, **Distribution Group** (***группы рассылки***). Объясняется это наличием ***групповых операций***, для которых *не нужно контролировать параметры безопасности.* Например, создание группы пользователей для распространения программного обеспечения или группы для централизованной рассылки почты. Отсутствие SID не мешает в этом случае правильному функционированию программ, но существенно снижает нагрузку операционной системы.

Группы могут ***иметь постоянных членов*** (каждый пользователь назначается в соответствующую группу администратором) или ***основываться на выборке пользователей по каким-либо правилам.*** Например, можно создать группу, в которую будут включаться пользователи с записью в их свойствах, что они работают в "отделе 22". Изменилось соответствующее поле в свойствах пользователя - и при очередных операциях с данной группой система произведет выборку пользователей, "увидит" новых членов группы и выполнит необходимые действия. Обратите внимание, что такие группы с динамическим членством не имеют SID, т.е. не могут быть использованы для контроля прав доступа.

Примечание

В Windows пользователь "получает" список групп, в которых он состоит, при входе в систему. Поэтому если администратор сменил у пользователя членство в группах, то это изменение начнет действовать только после нового входа в систему. Если пользователь должен быстро получить доступ к ресурсам, ему *следует завершить работу* в системе **(log off)** и сразу же вновь войти в неё **(log on).**

[3] При смене должности пользователя достаточно переместить его в другую группу. При создании новых проектов права доступа к ним будут назначаться на основе существующих групп и т. п.

Разрешения общего доступа и разрешения безопасности

Для объектов, предоставляемых в совместное использование, существуют два типа разрешений. Это разрешения ***общего доступа*** и ***разрешения безопасности***. (***Разрешения общего доступа*** *определяют право на использование данного ресурса при сетевом подключении.* Если у пользователя нет такого права (или это действие запрещено явно), то он просто не сможет подключиться к запрашиваемому ресурсу.

Разрешение безопасности - это разрешение на уровне прав доступа файловой системы. Оно существует при использовании файловой системы типа **NTFS** и проверяется *независимо от разрешений общего доступа*. Иными словами**,** если пользователю разрешено подключаться к этому ресурсу по сети, *доступ к файлам запрещен разрешениями безопасности*, то в итоге работа с такими файлами будет ***невозможна.*** Если на диске с ресурсами использована файловая система **FAT (FAT32)**, то доступ по сети будет контролироваться только *разрешениями общего доступа*.

Примечание

Типичной ошибкой пользователей, связанной с наличием двух типов разрешений, является предоставление в совместное, использование папок, находящихся на рабочем столе. После предоставления общего доступа к таким папкам другие пользователи не могут открыть файлы и т. п. Связана эта ***ошибка*** с тем, что **рабочий стол** - это папка в профиле пользователя. А разрешение безопасности на профиль пользователя по умолчанию разрешает доступ к нему *только этому пользователю и администратору компьютера*. Поэтому для возможности работы других пользователей с такой общей папкой необходимо добавить для них *разрешения безопасности* на уровне файловой системы.

Поскольку эти разрешения в определенной степени дублируют друг друга с точки зрения результата, то на практике их *обычно комбинируют* в зависимости от желаемых условий доступа.

–Права доступа ко всем объектам сетевого ресурса одинаковы для всех пользователей.

В этом случае разрешения общего доступа и разрешения безопасности выставляются *идентичными для всех заданных групп пользователей*.

–Права доступа различны для различных объектов сетевого ресурса

Разрешения общего доступа устанавливаются по максимально возможным правам. Так, если часть файлов должна быть *доступна только для чтения*, а часть и для редактирования, то ***разрешения общего доступа*** следует установить, как **"полный доступ"** *для всех групп пользователей*, которым ресурс должен быть доступен по сети. А разрешениями безопасности нужно выполнить *точную настройку*: **установить разрешение только для чтения для одних папок**, ***полный доступ*** - для других, запретить доступ к определенным папкам для некоторых групп пользователей и т. д. Такой подход упростит структуру ресурсов сети при сохранении всех необходимых разрешений.

Автоматически создаваемые учетные записи

При установке операционной системы автоматически создается несколько учётных записей пользователей. Ранее мы упоминали учетную запись **Администратор**. Эта учетная запись *особая*. Ранее ее нельзя [4]было даже у*далить* и *исключить из группы администраторов*. Сделано это было из *соображений безопасности, чтобы пользователь случайно не удалил всех администраторов, и система не стала неуправляемой.*

Учетная запись администратора представляет собой учетную запись пользователя, с помощью которой можно вносить изменения, затрагивающие других пользователей компьютера. Администраторы могут менять параметры безопасности, устанавливать программное обеспечение и оборудование, а также они имеют доступ ко всем файлам на компьютере. Кроме того,

[4] **В версиях, более ранних чем Windows XP. В новых версиях Windows упомянутые операции допустимы.**

администраторы могут изменять любые учетные записи пользователей. При установке Windows потребуется создать учетную запись пользователя. Она будет являться учетной записью администратора, позволяющей настраивать компьютер и устанавливать любые программы. После окончания настройки компьютера для повседневной работы рекомендуется использовать обычную учетную запись пользователя. Для большей безопасности рекомендуется применять обычную учетную запись вместо учетной записи администратора, поскольку в этом случае пользователи не могут вносить изменения, затрагивающие других пользователей компьютера.

Другая автоматически создаваемая учетная запись - это **Гость (Guest).** Она *не имеет пароля* и предназначена для обеспечения возможности работы с данным компьютером пользователя, у которого в системе нет учетной записи. *К* примеру, вы приезжаете со своим ноутбуком в другую организацию и хотите распечатать документ. Если в той организации принтер предоставлен в совместное использование и действует учетная запись Гость, то вы можете подключиться к принтеру и выполнить печать, в противном случае вам должны сообщить *имя входа* и *пароль*, которые можно использовать для подключения к *серверу печати*. В рабочих станциях Windows Server 4.0 эта учетная запись по умолчанию была доступна. В серверных операционных системах и в версиях рабочих станций, Windows 2000/XP/Vista/7 учетная запись **Гость** по соображениям безопасности **заблокирована**. Однако если ваша сеть полностью автономна и объединяет немного компьютеров, то для облегчения использования сетевых ресурсов вы *можете ее разблокировать*.

Так делает, например, мастер *конфигурирования домашней сети:* если вы определили, что компьютер используется в рамках домашней сети, то мастер разрешает использование учетной записи **Гость.** В этом случае, если вы разрешите *совместное использование ресурсов* компьютера, то к ним будет возможно *подключение любых пользователей*, независимо от того, существуют ли для них учетные записи на вашем компьютере или нет.

Учетная запись Система

При необходимости можно настроить службы для старта от *имени любого пользователя*. Однако в этом случае вам необходимо установить соответствующей учетной записи постоянный пароль и предоставить ей достаточно *большие права* по отношению к локальному компьютеру. Из такого сочетания требований очевидно вытекает настоятельная рекомендация: *не использовать учетные записи пользователей для запуска служб по соображениям безопасности.*

Учетная запись *Система* (Local System) предназначена для запуска служб компьютера. Она обладает *полными правами* по отношению к локальному компьютеру и фактически является частью операционной системы. Ее права существенно *выше, чем права любой учетной* записи пользователя. Для учетной записи **Система** выполняется *обход проверок безопасности*, поэтому для *нее не существует пароля, который можно было бы дешифровать или взломать*. Учетная запись **Система** не может быть использована *для доступа к сетевым ресурсам.*

Примечание

Следует быть внимательным при назначении прав доступа к локальным ресурсам компьютера. Можно столкнуться с ситуацией, когда недостаточно опытные пользователи, желая ограничить доступ к ресурсам своего компьютера, работающего в составе сети, запрещали доступ к файлам на диске всем, кроме самого себя. Исключив специальных пользователей, они *сделали невозможным запуск многих служб*, необходимых для работы операционной системы.

Встроенные группы

При установке операционной системы на компьютере автоматически создается несколько групп. Для большинства случаев персонального использования этих групп достаточно для безопасной работы и управления системой.

– **Администраторы (Administrators).**

Члены этой группы имеют *все права* на управление компьютером. После установки в системе присутствуют только пользователи-члены этой группы (в Windows XP в ходе установки можно создать *несколько администраторов* системы, в предыдущих версиях создается только одна запись).

– **Пользователи (Users).**

Это основная группа, в которую надо включать обычных пользователей системы. Членам этой группы *запрещено выполнять операции, которые могут повлиять на стабильность и безопасность работы компьютера.*

– **Гости (Guests).**

Эта группа объединяет пользователей, для которых действуют специальные права для *доступа «чужих»* пользователей. По умолчанию в нее включена только одна заблокированная учетная запись **Гость.**

Практическая часть

Вопрос 1. Установка разрешений на доступ к файлам и папкам

На уровне файловой системы безопасность Windows чаще всего обеспечивается за счет предоставления так называемых ***разрешений на доступ к файлам и папкам***. Эти разрешения указывают, разрешено ли пользователю или группе получать доступ к тому или иному файлу либо папке, и если да, то *что конкретно позволено делать с этим файлом или папкой.* Например, *одному* пользователю может быть разрешен только просмотр содержимого файла или папки, а *другому* - также и внесение изменений.

В Windows предлагается ***набор стандартных разрешений***, **шесть** из которых допускается устанавливать **на уровне папок** и **пять** - **на уровне файлов.**

Виды стандартных разрешений.

1) **Полный доступ.** Позволяет ***пользователю*** или ***группе*** выполнять *любое из действий*, которые перечисляются далее, а также *изменять разрешения.*

2) **Изменение.** Позволяет ***пользователю*** или ***группе*** *просматривать содержимое файлов или папок, открывать файлы, редактировать их, создавать новые файлы и подпапки, а также удалять файлы и запускать программы.*

3) **Чтение и выполнение.** Позволяет ***пользователю*** или ***группе*** *просматривать содержимое файла или папки, открывать файлы и выполнять программы.*

4) **Список содержимого папки.** Может предоставляться только ***на уровне папок*** и позволяет ***пользователю*** или ***группе*** просматривать *содержимое соответствующей папки*.

5) **Чтение**. Позволяет ***пользователю*** или ***группе*** *открывать файлы*, но ***не редактировать*** их.

6) **Запись.** Позволяет пользователю *создавать новые файлы и подпапки*, а также *открывать и редактировать существующие файл*ы.

Вдобавок предлагается довольно *длинный* ***перечень*** так называемых ***особых разрешений***, которые позволяют *более точно настраивать доступ к папкам и файлам* (и которые подробно рассматриваются далее).

Чаще всего разрешения предоставляются с помощью встроенные **групп безопасности**. Для каждой такой группы настраивается *конкретный набор разрешений* и *прав*, после чего каждый добавляемый в нее пользователь ***автоматически*** получает только ассоциируемые с ней разрешения и права.

Таблица 1 - Две основные группы безопасности

Администраторы	Членам этой группы предоставляется полный контроль над компьютером, а это значит, что им разрешено **делать следующее:** получать доступ ко всем папкам и файлам; устанавливать и удалять программы (включая унаследованные программы) и устройства; создавать, изменять и удалять учетные записи пользователей; устанавливать обновления Windows, пакеты программ и средства, обеспечивающие совместимость приложений; использовать безопасный режим; восстанавливать систему Windows; менять владельцев объектов и многое другое.

Пользователи	Членам этой группы (также называемым **стандартными пользователями**) разрешено получать доступ только к тем файлам, которые хранятся в ***их собственных папках или папках, являющихся совместно используемыми*** на данном компьютере; *изменять пароль и рисунок для своей учетной записи; запускать и устанавливать программы, не требующие наличия, прав администратора.*

Помимо этих ***групп***, в Windows также поставляется *около* ***десятка других***, которые применяются *реже*. Важно обратить внимание на то, что разрешения, назначаемые этим группам, также ***автоматически*** *назначаются и членам группы* **Администраторы.** Это означает, что если у пользователя имеется учетная запись **администратора**, ему *не нужно также быть членом никакой другой группы* для того, чтобы выполнять задачи, являющиеся *специфическими* для данной группы. Все эти ***дополнительные группы*** перечислены ниже.

Примечание

Обратите внимание, что после использования мастера установки Windows в режиме отображения страницы приветствий во время входа в систему название учетной записи администратора *не показано* на экране. Однако эта учетная запись *может быть применена для работы с системой*, причем обычно администраторы ***забывают о необходимости установки для нее пароля***, что позволяет легко локально зайти в систему с правами администратора, предъявив "пустой" пароль.

Целесообразно назначить этой учетной записи ***длинный и сложный пароль, состоящий из цифр и символов только английского алфавита.*** Это упростит возможные операции по восстановлению операционной системы. Кроме того, в *целях безопасности* рекомендуется *переименовать* ***учетные записи администраторов*** и ***запретить для анонимных пользователей просмотр базы идентификаторов безопасности.***

Опытные пользователи могут использовать сценарии **Visual Basic** для автоматизации типовых операций с учетными записями.

1.1 Добавление пользователя в группу безопасности

Преимущество подхода с использованием **групп безопасности** для предоставления *разрешений* состоит в том, что после настройки для *группы прав доступа* файлу или папке больше изменять параметры безопасности для этого объекта *не потребуется*. Вместо этого *любые новые пользователи*, которые *создаются* и *добавляются* в соответствующую группу безопасности, ***автоматически*** получают разрешения, которые были установлены для этой группы.

Шаги, необходимые для добавления пользователя в конкретную группу безопасности в Windows.

1. Щелкните на кнопке **Пуск**, ***введите командная строка***, в списке результатов поиска щелкните правой кнопкой мыши на варианте **Командная строка** и выберите в контекстном меню пункт **Запуск от имени администратора.** Появится диалоговое окно **Контроль учетных записей пользователей.** Введите в окне **Контроль учетных записей пользователей свои учетные данные.**
2. Введите в окне командной строки команду **control userpasswords2**.
3. Щелкните на кнопке **ОК.** Появится диалоговое окно **Учетные записи пользователей** (рисунок 1).

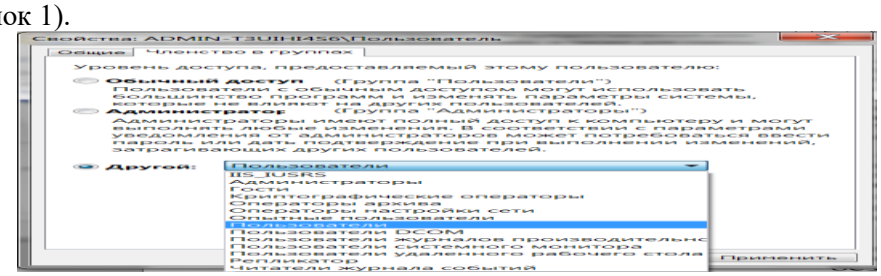

Рисунок 1 - Диалоговое окно **Учетные записи пользователей** позволяет добавлять пользователей в *любую из поддерживаемых* в Windows групп безопасности

4. Выделите нужного пользователя и щелкните на кнопке **Свойства.** Появится ***ведомость свойств*** этого пользователя.
5. Перейдите на вкладку **Членство в группах**.
6. Установите переключатель **Другой** и затем выберите желаемую группу безопасности в предлагаемом списке.
7. Щелкните на кнопке **ОК.**

Задание 1. Создать учётную запись пользователя со своим именем и добавить его в группу «Пользователи»

1.2 Добавление пользователя сразу в несколько групп безопасности

При желании добавить пользователя в более чем одну группу безопасности, следует знать, что подход с диалоговым окном **Учетные записи пользователей**, описанный в предыдущем разделе, работать *не будет.* Те, у кого установлена версия Windows **Ultimate (Windows Максимальная), Enterprise (Windows Корпоративная),** или **Professional (Windows Профессиональная)**, могут использовать для добавления пользователя *сразу в несколько групп оснастку* **Локальные пользователи и группы.** Ниже перечислены необходимые шаги.

Щелкните на кнопке **Пуск**, введите команду **lusrmgr.msc** и нажмите клавишу **<Enter>.** Появится окно оснастки **Локальные пользователи и группы.**

Дважды щелкните на нужном пользователе. Появится ***ведомость свойств*** этого пользователя.

Перейдите на вкладку **Членство в группах.**

Щелкните на кнопке **Добавить**. Windows отобразит диалоговое окно **Выбор: "Группы".**

Если имя нужной группы точно известно, *введите его* в большом текстовом поле, а если ***нет***, тогда щелкните на кнопке **Дополнительно**, а потом на *кнопке* **Поис**к, после чего дважды щелкните на имени интересующей группы в списке, который появится **Далее**.

Повторите шаг 5 для выбора *других групп*, в которые требуется добавить пользователя.

Щелкните на кнопке **ОК**. На вкладке **Членство в группах** появится список всех выбранных групп, как показано на рисунок 2.

Щелкните на кнопке **ОК**. Windows добавит пользователя во все эти группы *сразу же*, как только этот пользователь войдет в систему в следующий раз.

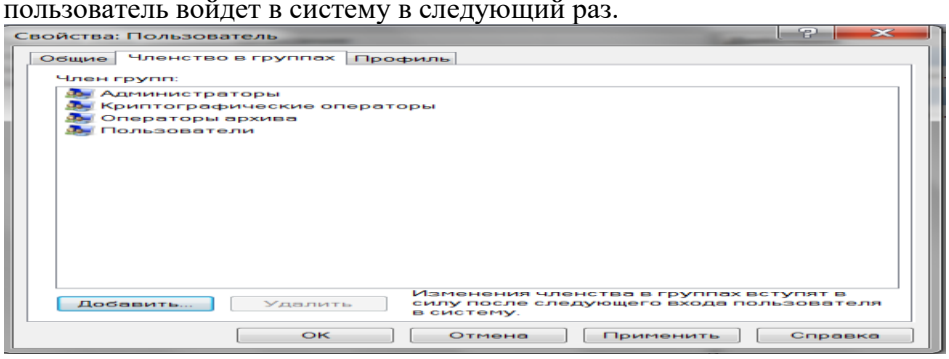

Рисунок 2 - Для добавления пользователя сразу в несколько групп безопасности можно использовать оснастку **Локальные пользователи и группы**

Если файловая система на компьютере преобразована в **NTFS**, то **дополнительно** появляется возможность контролировать доступ к отдельным файлам и папкам**,** определяя соответствующие права доступа.

Права пользователей назначаются через оснастку **Локальная безопасность**, расположенную в группе административных **задач.**

Задание 2. Добавить учётную запись пользователя в несколько групп безопасности**: Криптографические операторы, Операторы настройки сети, Операторы архива, Опытные пользователи.**

1.3 Предоставление стандартных разрешений

Шаги, необходимые для предоставления ***пользователю*** или ***группе*** любых ***стандартных разрешений***, которые описывались ранее.

Выглядят следующим образом:

1. Отобразите в окне проводника Windows файл или папку, которую *требуется защитить.*

2. Щелкните на этом файле или папке правой кнопкой мыши и выберите в контекстном меню пункт **Свойства** (или, если папка уже открыта, щелкните на кнопке **Упорядочить** и

выберите пункт **Свойств** в открывшемся меню).

3. Перейдите на вкладку **Безопасность.**

4. Щелкните на кнопке **Изменить.** Откроется диалоговое окно **Разрешения для группы "X"**, где на месте **X** будет идти ***имя соответствующего файла или папки.***

5. Щелкните на кнопке **Добавить**, чтобы открыть диалоговое окно Выбор: **"Пользователи"** или **"Группы".**

6. Если *точно известно имя* нужного пользователя или группы, введите его в большом текстовом поле, а если нет, тогда щелкните на кнопке **Дополнительно**, потом на кнопке **Поиск** и затем дважды на имени интересующего ***пользователя*** или ***группы в списке***, который появится **Далее**.

7. Щелкните на кнопке **ОК**. Снова появится диалоговое окно **Разрешения для группы "X"**, но только на этот раз в нем будет отображаться ***имя нового добавленного пользователя*** или ***группы***.

8. С помощью полей для установки отметки в столбцах **Разрешить и Запретить** предоставьте желаемые разрешения этому пользователю или группе, как показано на рисунке 3.

9. Щелкните на кнопке **ОК** во всех открытых диалоговых окнах.

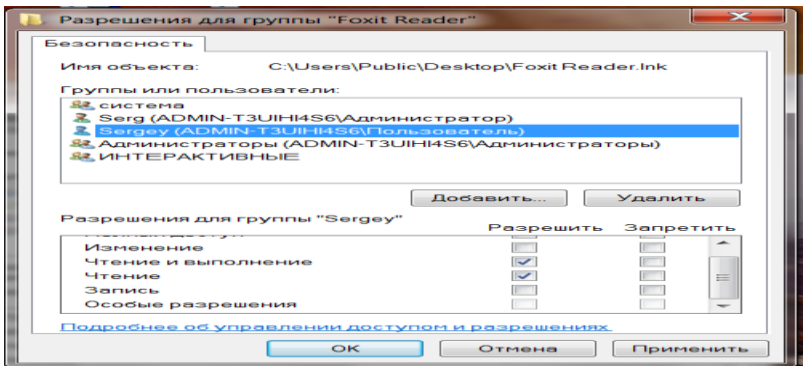

Рисунок 3 - Предоставишь *стандартные разрешения* пользователю или группе можно путем открытия для интересующего файла или папки диалогового окна **Разрешения**

Задание 3. Создайте папку и два текстовых файла. Назовите их своим именем с номерами 1 и 2 соответственно. Предоставьте учётной записи пользователя стандартное разрешение к файлу User_1 на Полный доступ и файлу User_2 разрешение на чтение.

1.4 Предоставление особых разрешений

В некоторых ситуациях может потребоваться предоставить ***пользователю*** или ***группе*** более конкретные разрешения, например, позволить *добавлять новые файлы в папку*, но ***не новые подпапки***, или предоставить ***полный доступ к файлу или папке***, но лишить возможности *изменять разрешения* или *становиться владельцем объекта*.

Для таких конкретных случаев в Windows предлагается ***набор особых разрешений,*** **14** из которых могут предоставляться на уровне ***папок*** и **13** - на уровне ***файлов***.

Список особых разрешений

1) **Полный доступ.** Позволяет пользователю или группе выполнять *любое из действий*, которые описаны ниже.

2) **Траверс папок/выполнение файлов.** Позволяет пользователю или группе *открывать папку для получения доступа к другой папке* или выполнять программный файл.

3) **Содержание папки/чтение данных.** Позволяет пользователю или группе *просматривать содержимое папки* или *читать содержимое файла*.

4) **Чтение атрибутов.** Позволяет ***пользователю*** или ***группе*** просматривать атрибуты *папок или файлов* наподобие атрибута ***Только чтение*** *или* ***Скрытый.***

НА ЗАМЕТКУ

Для просмотра атрибутов файла или папки щелкните на интересующем файле или папке правой кнопкой мыши, выберите в контекстном меню пункт **Свойства** и перейдите на вкладку **Общие**.

5) **Чтение дополнительных атрибутов**. Позволяет ***пользователю*** или ***группе*** просматривать *дополнительные атрибуты папок или файлов* (которые присваиваются им

определенными программами).

6) **Создание файлов/запись данных.** Позволяет ***пользователю*** или ***группе*** *создавать новые файлы внутри папки или вносить изменения в файл.*

7) **Создание папок/дозапись данных.** Позволяет ***пользователю*** или ***группе*** создавать *новые подпапки внутри папки или добавлять новые данные в конец файла* (но ***не изменять*** существующие данные в нем).

8) **Запись атрибутов.** Позволяет ***пользователю*** или ***группе*** изменять ассоциируемые с папкой или файлом *атрибуты.*

9) **Запись дополнительных атрибутов.** Позволяет ***пользователю*** или ***группе*** вносить изменения в ассоциируемые с папкой или файлом *дополнительные атрибуты.*

10) **Удаление подпапок и файлов.** Может предоставляться только на *уровне папок* и позволяет ***пользователю*** или ***группе*** *удалять подпапки* или *файлы*, содержащиеся *внутри* соответствующей папки.

11) **Удаление.** Позволяет ***пользователю*** или ***группе*** *удалять папки или файлы.*

12) **Чтение разрешений.** Позволяет ***пользователю*** или ***группе*** просматривать *разрешения*, ассоциируемые с папкой или файлом.

13) **Смена разрешений.** Позволяет ***пользователю*** или ***группе*** *редактировать разрешения*, ассоциируемые с папкой или файлом.

14) **Смена владельца.** Позволяет ***пользователю*** или ***группе*** *менять владельца* папки или файла.

Шаги, необходимые для предоставления особых разрешений на уровне того или иного файла или папки.

1) Отобразите в окне проводника Windows ***файл*** или ***папку***, которую *требуется защитить.*

2) Щелкните на этом файле или папке правой кнопкой мыши и выберите в контекстном меню пункт **Свойства** (или, если папка уже открыта, щелкните на кнопке **Упорядочить** и выберите пункт **Свойств** в открывшемся меню).

3) Перейдите на вкладку **Безопасность.**

4) Щелкните на кнопке **Дополнительно.** Появится диалоговое окно **Дополнительные параметры безопасности для "X"**, где на месте **X** будет идти имя соответствующего файла или папки.

5) Щелкните на вкладке **Разрешения** на кнопке **Изменить разрешения**.

6) Выделите существующее разрешение, которое необходимо изменить.

7) Щелкните на кнопке **Изменить.** Появится диалоговое окно **Элемент разрешения для "X".**

8) С помощью полей для отметок в столбцах **Разрешить** и **Запретить** предоставьте желаемые разрешения данному пользователю или группе, как показано на рис. 17.4.

9) Щелкните на кнопке **ОК** во всех открытых диалоговых окнах.

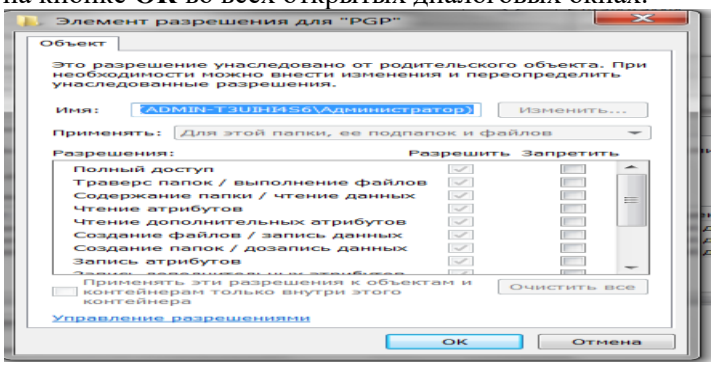

Рисунок 4 - С помощью диалогового окна **Элемент разрешения для "X"** можно предоставлять пользователю или группе *особые разрешения*

Задание 4. Предоставьте учётной записи пользователя особые разрешения к файлу **User_1** запретить **Смену разрешений** к файлу **User_2** запретить разрешение на чтение атрибутов.

Вопрос 2. Шифрование файлов и папок

Если злоумышленник *не может войти в* Windows, означает ли это, что данные находятся в безопасности? К сожалению, нет; скорее всего, им все равно грозит опасность.

В случае, если взломщик получит физический доступ к ПК, либо проникнув в офис, либо украв компьютер, он сможет с помощью *специальных утилит просмотреть содержимое*

*жесткого диск*а. Это означает, что если на компьютере хранятся какие-то *чрезвычайно важные или конфиденциальные данные*, наподобие личных *финансовых файлов, медицинских карт, сведений о зарплате сотрудников компании, торговых секретов, производственных планов, журналов или дневников,* для злоумышленника не представит особого труда прочитать и даже скопировать их.

Для тех, кого беспокоит вероятность просмотра кем-либо *приватных файлов*, Windows предоставляется возможность шифровать содержащуюся в файлах информацию так, чтобы она выглядела совершенно непонятно для всех кроме владельца данной учетной записи в Windows. После шифрования файлов пользователь может работать с ними совершенно так же, как и раньше, *без какой-либо заметной потери производительности.*

НА ЗАМЕТКУ

Для применения шифрования к файлам необходимо, чтобы на жестком диске была обязательно установлена файловая система **NTFS**. Чтобы узнать, какая файловая система установлена на диске в текущий момент, щелкните на кнопке **Пуск**, выберите пункт **Компьютер**, затем выделите в окне **Компьютер** интересующий диск и просмотрите информацию о файловой системе в панели сведений. При необходимости преобразовать файловую систему на диске в **NTFS** щелкните на кнопке **Пуск**, введите в поле поиска строку командная строка, в списке результатов щелкните правой кнопкой мыши на варианте Командная строка и выберите в контекстном меню команду **Запуск от имени администратора.**

Введите в окне командной строки команду **convert d: /fs:ntfs**
с указанием на месте **d** буквы диска, который подлежит преобразованию, и нажмите клавишу <**Enter**>. Если Windows предложит размонтировать том, нажмите <**Y**>, а затем <**Enter**>.

2.1 ***Действия, которые понадобится предпринять для шифрования важных данных.***

1. С помощью **проводника Windows** найдите значок папки, в которой содержатся подлежащие шифрованию данные.

СОВЕТ

Хотя допускается шифровать и отдельные файлы, лучше все-таки зашифровать сразу целую папку, поскольку тогда Windows будет автоматически шифровать и любые новые файлы, которые будут в нее добавляться.

2. Щелкните правой кнопкой мыши на значке этой папки и выберите в контекстном меню пункт **Свойства**, чтобы открыть ведомость свойств этой папки.
3. Перейдите на вкладку **Общие.**
4. Щелкните на кнопке **Другие.** Откроется диалоговое окно **Дополнительные атрибуты.**
5. Установите *отметку* рядом с опцией **Шифровать содержимое для защиты данных.**
6. Щелкните на кнопке **ОК** в каждом из открытых диалоговых окон. Откроется диалоговое окно **Подтверждение изменения атрибутов.**
7. Выберите в этом окне переключатель **К данной папке и ко всем вложенным папкам и файлам.**
8. Щелкните на кнопке **ОК.** После этого Windows произведет шифрование содержимого данной папки.

СОВЕТ

По умолчанию имена всех зашифрованных файлов и папок выделяются в Windows ***зеленым цветом***, что помогает отличать их от *незашифрованных файлов* и *папок*. Если имена зашифрованных файлов и папок *не должны выделяться*, откройте окно любой папки, щелкните на кнопке **Упорядочить**, выберите в появившемся далее меню пункт **Параметры папок и поиска**, перейдите на вкладку **Вид**, снимите отметку с опции **Отображать сжатые или зашифрованные файлы NTFS другим цветом** и щелкните на кнопке **ОК**.

Задание 5. С помощью **проводника Windows** найдите значок своей папки, в которой содержатся подлежащие шифрованию данные. Зашифровать содержимое данной папки и все вложенные файлы для защиты данных, а также снять их выделение цветом.

Вопрос 3. Шифрование диска с помощью BitLocker

В случае использования, предлагаемых в Windows ***технологий защиты***, таких как *двухсторонний* **брандмауэр Windows**, программа **"Защитник Windows"** и компонент

Windows Service Hardening (Повышение стойкости служб Windows), хороших *политик в плане управления заплатами* (т.е. применения заплат безопасности сразу же *после их появления*) и небольшого количества здравого смысла, у зловредного ПО не должно оставаться никакого шанса на проникновение в компьютер, на котором работает Windows.

Но как на счет того, когда Windows не работает?

В случае *кражи компьютера или проникновения злоумышленника в дом, или офис*, безопасность системы может нарушаться **двумя разными способами.**

1) За счет загрузки **с диска** и сброса пароля администратора посредством специальных ***утилит командной строки***.

2) За счет использования загружаемой с компакт-диска ***операционной системы*** для получения доступа к жесткому диску и затем ***сброса всех разрешений, которые установлены на уровне папок и файлов.***

Любой из этих способов позволяет злоумышленнику получить доступ к содержимому компьютера. В случае хранения на компьютере секретных данных, например, важной финансовой информации, конфиденциальных материалов компании и т.п., результаты могут оказаться просто катастрофическими.

Для оказания помощи с предотвращением возможности доступа к важным секретным данным со стороны злоумышленников, в Windows поставляется технология под названием **BitLocker**, которая позволяет ***шифровать содержимое сразу всего диска***. В таком случае, даже при получении злоумышленником *физического доступа* к компьютеру, прочитать содержимое диска не удастся. Действие **BitLocker** основано на ***сохранении специальных ключей***, позволяющих *шифровать* и *дешифровать* секторы на системном диске в ***микросхеме*** **TPM (Trusted Platform Module)** 1.2, которая представляет собой ***аппаратный компонент***, доступный на многих современных машинах.

НА ЗАМЕТКУ

Чтобы узнать, установлена ли на компьютере микросхема **TPM**, перезагрузите систему, получите доступ к параметрам **BIOS** (обычно, нажав <**Delete**> или какую-то другую клавишу), а затем (в большинстве случаев) найдите раздел с названием наподобие **Security** и выясните, присутствует ли в нем запись TPM.

3.1 Включение BitLocker в системе с TPM

Для включения **BitLocker** в системе, которая поставляется с **TPM**, щелкните на кнопке **Пуск**, выберите пункт **Панель управления**, перейдите в раздел **Система и безопасность**, а затем в подраздел **Шифрование диска BitLocker**. В окне **Шифрование Диска BitLocker**, которое показано на рисунке 5, щелкните на ссылке **Включить BitLocker** напротив нужного жесткого диска.

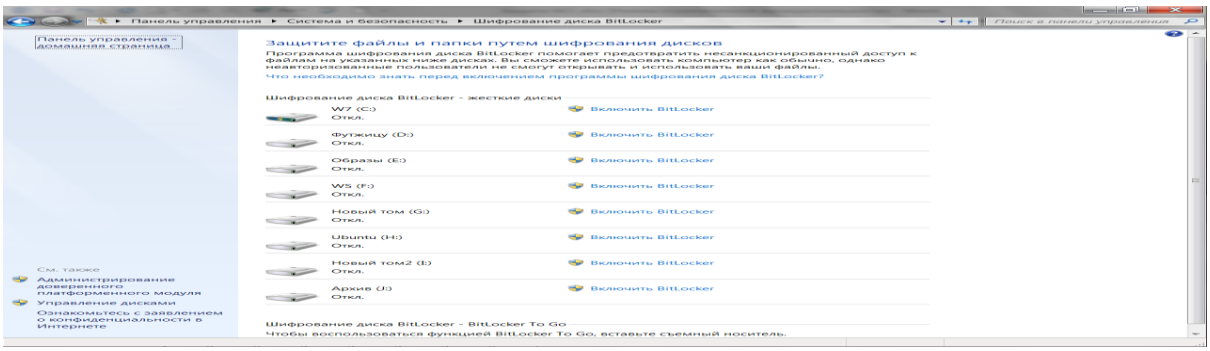

Рисунок 5 - С помощью окна Шифрование диска **BitLocker** можно включать и отключать программу шифрования **BitLocker** для конкретного диска

НА ЗАМЕТКУ

Для работы с установленной на компьютере микросхемой **TPM** можно также использовать оснастку **"Управление доверенным платформенным модулем (TPM) на локальном компьютере"**. Чтобы получить доступ к этой оснастке, нажмите одновременно клавишу с логотипом **Windows** и клавишу **<R>**, введите команду **tpm.msc** и щелкните на кнопке **ОК**. С помощью этой оснастки *можно просматривать сведения о текущем состоянии модуля* **TPM**, *получать информацию о его производителе и выполнять связанные с его управлением операции.*

Включение BitLocker в системе без TPM

Даже если на компьютере *не установлена микросхема* **TPM**, программу **BitLocker** все равно можно использовать. В этом случае понадобится сохранить загрузочный ***ключ* BitLocker** на подключаемой через **USB-порт флэш-карте** и затем вставлять эту карту при каждом запуске компьютера для расшифровки содержимого диска и получения возможности работать с компьютером обычным образом.

Однако предварительно потребуется сконфигурировать Windows так, чтобы она позволяла использовать **BitLocker** в системе **без TP**M. Ниже перечислены необходимые шаги.

1. Щелкните на кнопке **Пуск**, введите в поле поиска **gpedit.msc** и нажмите клавишу **<Enter>**, чтобы отобразить окно ***редактора локальной групповой политики.***
2. Последовательно откройте папки **Конфигурация компьютера**, **Административные шаблоны, Компоненты Windows, Шифрование диска BitLocker** и **Диски операционной системы**.
3. Дважды щелкните на политике **Обязательная дополнительная проверка подлинности при запуске.**
4. Выберите переключатель **Включить.**
5. Установите отметку рядом с опцией **Разрешить использование BitLocker без совместимого TPM**, как показано на рис. 17.6.
6. Щелкните на кнопке **ОК.**
7. Чтобы заставить Windows привести новую политику в действие немедленно, щелкните на кнопке **Пуск,** введите команду **gpupdate /force** и нажмите клавишу **<Enter>.**

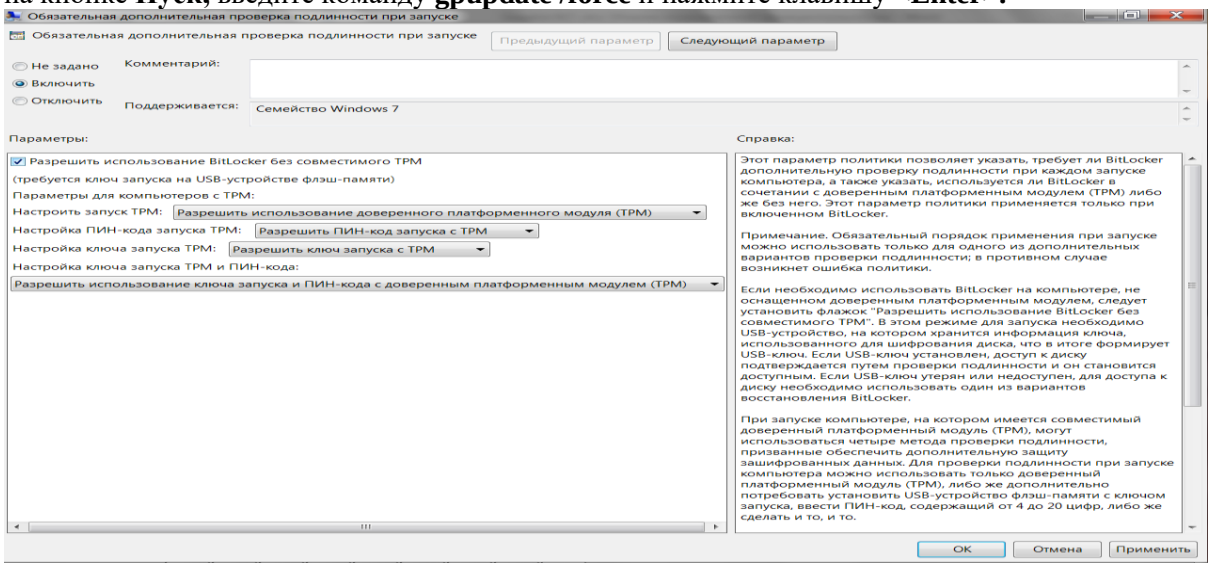

Рисунок 6 - Для настройки Windows так, чтобы она позволяла использовать **BitLocker без TPM**, применяется политика **Обязательная дополнительная проверка подлинности** при запуске

НА ЗАМЕТКУ

Если в версии Windows редактор локальной групповой политики отсутствует, настроить **BitLocker на работу в системе без TPM** можно за счет редактирования системного реестра. В этом случае понадобится создать и сконфигурировать в системном реестре новый раздел и несколько новых параметров. Для упрощения данной задачи на сайте издательства доступен для загрузки *файл*, позволяющий сделать это автоматически.

Для включения BitLocker выполните следующие действия.

1. Выберите в меню **Пуск** пункт **Панель управления →Система и**

безопасность→Шифрование диска BitLocker, чтобы открыть окно **Шифрование диска BitLocker.**

2. Щелкните на ссылке **Включить BitLocker** напротив нужного диска. Откроется окно *мастера шифрования диска* **Bitlocker.**

3. Щелкните на кнопке **Далее.** Мастер сообщит о том, что для включения **BitLocker** будет использован *существующий диск* или *свободное пространство на системном диске*.

4. Щелкните на кнопке **Далее**. **Мастер** подготовит жесткий и предложит *перезагрузить систему*.

5. Щелкните на кнопке **Перезагрузить сейчас**. Компьютер перезагрузится, и по возвращении в Windows на экране снова появится окно *мастера*.

6. Щелкните на кнопке **Далее.** Появится диалоговое окно **Задать параметры запуска BitLocker.**

7. *Выберите вариант* **Запрашивать ключ запуска** при запуске и щелкните на кнопке **Далее.**

8. Вставьте **флэш-карту USB**, на которой должен быть сохранен ***ключ*** запуска **BitLocker.**

9. Выберите в *списке устройств эту карту* и затем щелкните на кнопке **Сохранить**. После этого *мастер* спросит о том, как следует *сохранить ключ восстановления*.

10. Выберите один из следующих вариантов, после чего щелкните на кнопке **Далее.**

– **Сохранить ключ восстановления на флэш-накопителе USB.** Этот вариант позволяет *сохранять ключ восстановления на флэш-карте* и является, пожалуй, *наилучшим*, поскольку означает *возможность восстановления файлов* просто путем вставки соответствующей флэш-карты. Вставьте флэш-карту, выберите ее в появившемся после этого списке и щелкните на кнопке **Сохранить.**

– **Сохранить ключ восстановления в файле.** Этот вариант позволят сохранять ключ восстановления на *отдельном жестком диске* в системе. Укажите желаемое место для сохранения ключа в диалоговом окне **Сохранить ключ BitLocker как** и щелкните на кнопке **Сохранить.**

– **Напечатать ключ восстановления.** Этот вариант позволяет ***распечатать*** *ключ восстановления*. Выберите желаемый принтер в открывшемся диалоговом окне и щелкните на кнопке **Печать.**

11. Щелкните на кнопке **Продолжить.** После этого **BitLocker** сообщит о необходимости перезапустить систему.

12. Если был выбран вариант сохранения ключа восстановления на флэш-карте **USB**, вставьте эту карту (если она еще *не вставлена*) и щелкните на кнопке **Перезагрузить сейчас.**

13. После перезагрузки компьютера **BitLocker** начнет *шифрование диска* и в области уведомлений появится соответствующее информирующее об этом сообщение, на котором при желании можно щелкнуть и наблюдать *за ходом процесса шифрования*.

Задание 5. Выполнить шифрование диска с помощью **BitLocker.** Проверить включен ли **BitLocker** в системе с TPM на Вашем компьютере. Использовать оснастку **"Управление доверенным платформенным модулем (TPM) на локальном компьютере".** Включить **BitLocker в системе без TPM** и сохранить загрузочный ***ключ*** **BitLocker** на подключаемой через **USB-порт флэш-карте.** Привести новую политику в действие. С сайта издательства загрузить *файл* настройки **BitLocker на работу в системе без TPM** без локальной групповой политики за счёт редактирования системного реестра. Создать и сконфигурировать в системном реестре новый раздел и новые параметры. Сохранить ключ восстановления на флэш-накопителе **USB,** в файл и напечатать**.**

Контрольные вопросы

1) Для чего предназначена учётная запись, хранимая в компьютерной системе и какие сведения она содержит?
2) Какие сведения может содержать учётная запись дополнительно?
3) Что применяется для доступа к учетной записи?
4) Сколько существует типов учётных записей и почему?
5) В чём заключается отличительная особенность профессиональных версий ОС Windows?
6) Каким образом операционная система различает «различает» пользователей?

7) Что такое SID и для чего он предназначен?
8) Могут ли создаваться две учётных записи с одинаковы номером?
9) Сколько существует типов учётных записей при работе в компьютерной сети?
10) Как осуществляется назначение права доступа к папке для нескольких десятков сотрудников в средней организации?
11) Когда начнет действовать изменение если администратор сменил у пользователя членство в группах и почему?
12) Для чего служат разрешения общего доступа?
13) Для чего служат разрешение безопасности?
14) Какое разрешение доступа будет действовать если на диске с ресурсами использована файловая система FAT (FAT32)?
15) Какое разрешение доступа других пользователей будет действовать если при использование папок, находящихся на рабочем столе?
16) Какие учетные записи создаются автоматически и для чего они предназначены?
17) Для чего предназначена учетная запись Система и какими правами она обладает?
18) Какие на компьютере группы создаются автоматически?
19) Каким образом установить разрешение на доступ к файлам и папкам?
20) Какие виды стандартных разрешений?
21) Каким образом добавить пользователя в группу безопасности?
22) Каким образом добавление пользователя сразу в несколько групп безопасности?
23) Каким образом предоставить стандартных разрешения?
24) Каким образом предоставить особые разрешения?
25) Сколько всего особых разрешений в ОС Windows?
26) Каким образом осуществляется шифрование файлов и папок?
27) Каким образом осуществляется шифрование диска с помощью BitLocker?
28) Каким образом может осуществляется безопасность системы?
29) Каким образом узнать установлена ли на компьютере микросхема TPM?
30) Для чего предназначена микросхема TPM?
31) Какие существуют варианты сохранения паролей в BitLocker?

Требования к форме и содержанию отчёта

Результаты лабораторной работы должны быть представлены в виде типовой отчетной документации по защите файловой системы. В качестве выводов должны быть представлен анализ проделанной работы и предложения по применению использованных средств защиты.