МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ им. Н.Э. БАУМАНА
Факультет «Информатика и системы управления»
Кафедра «Автоматизированные системы обработки информации и управления»

Сёмкин П.С., Сёмкин А.П.

Методические указания по выполнению лабораторных работ
по дисциплине
«Операционные системы»

Лабораторная работа № 7-8

«Администрирование параметров безопасности ОС Windows 7»

Москва
2017 г.

ОГЛАВЛЕНИЕ

1 Цель работы

Целью работы является знакомство с администрированием параметров безопасности операционной системы Windows 7.

Продолжительность работы – 4 часа.

2 Теоретическая часть

2.1 *Политики безопасности*

Компоненты, обеспечивающие безопасность, являются одними из важнейших в современных операционных системах. Обычно по умолчанию

компоненты ОС настроены для обеспечения среднего для обычного пользователя уровня безопасности.

Но иногда такого уровня безопасности оказывается недостаточно, и операционная система настраивается таким образом, чтобы обеспечивалась максимальная безопасность, даже ценой снижения производительности системы.

В операционной системе Windows имеется множество компонентов, отвечающих за ее безопасность. С помощью групповых политик можно получить доступ практически ко всем параметрам безопасности системы.

Основная часть этих политик расположена в оснастке ***Политика «Локальный компьютер»***.

За безопасность отвечают политики, расположенные в узле

Политика «Локальный компьютер» \ Конфигурация компьютера \ Конфигурация Windows \ Параметры безопасности

2.2 *Шифрование файлов, папок и дисков*

Для различных криптографических операций — шифрования данных на электронных носителях информации, создания и использования электронных цифровых подписей и шифрования пакетов данных при передаче по закрытым каналам связи, аутентификации пользователей используются криптосистемы с открытым ключом.

В таких системах используют два ключа шифрования - **открытый**, используемый для шифрования данные или проверки достоверность электронной подписи, и **закрытый**, позволяющий расшифровать данные или подписать их электронной подписью.

В операционной системе Windows такие ключи называют **сертификатами открытого и закрытого ключей,** поскольку такие ключи обычно подписаны электронной подписью центра сертификации.

Шифрующая файловая система позволяет пользователям зашифровывать принадлежащие им папки и отдельные файлы, расположенные на томах с файловой системой NTFS.

Для шифрования файла или папки следует просто установить для них атрибут **Шифровать содержимое для зашиты**. Если пометить папку как зашифрованную, то будут зашифрованы все файлы в этой папке, а все новые файлы, перемещенные в эту папку или созданные в ней, также будут зашифрованы.

Зашифрованные таким образом файлы в обычных условиях невозможно просмотреть другому пользователю, даже наделенному полномочиями администратора. При этом пользователь, зашифровавший файлы, может работать с ними как с обычными файлами. В результате применения шифрования, даже если компьютер будет украден или перезагружен в системе MS-DOS, файлы останутся нечитаемыми.

Когда пользователь сообщает системе, что хочет зашифровать определенный файл, формируется случайный 128-разрядный ключ.

Ключ используется для поблочного шифрования файла с помощью симметричного алгоритма, параметром в котором используется этот ключ.

Каждый новый шифруемый файл получает новый случайный 128-разрядный ключ, так что никакие два файла не используют один и тот же ключ шифрования, что увеличивает защиту данных в случае, если какой-либо из ключей окажется скомпрометированным.

Независимое шифрование каждого блока файла необходимо для сохранения возможности произвольного доступа к блокам файла.

Чтобы файл мог быть впоследствии расшифрован, ключ файла должен где-то храниться. Если бы ключ хранился на диске в открытом виде, тогда злоумышленник, укравший файлы, мог бы легко найти его и воспользоваться им для расшифровки украденных файлов. В этом случае сама идея шифрования файлов оказалась бы бессмысленной. Поэтому ключи файлов сами должны храниться на диске в зашифрованном виде. Для этого и используется шифрование с открытым ключом.

Открытый ключ можно без каких-либо опасений хранить прямо в реестре, так как по открытому ключу невозможно определить закрытый ключ,

необходимый для расшифровки файлов. Затем случайный 128-разрядный ключ файла шифруется открытым ключом, а результат сохраняется на диске вместе с файлом.

Чтобы расшифровать файл, с диска считывается зашифрованный случайный 128-разрядный ключ файла. Однако для его расшифровки необходим закрытый ключ. В идеале этот ключ должен храниться на смарт-карте, вне компьютера, и вставляться в считывающее устройство только тогда, когда требуется расшифровать файл. Хотя операционная система Windows поддерживает смарт-карты, она не позволяет хранить на них закрытые ключи.

Вместо этого, когда пользователь в первый раз зашифровывает файл с помощью системы EFS, операционная система Windows формирует пару ключей (закрытый ключ, открытый ключ) и сохраняет закрытый ключ, зашифрованный при помощи симметричного алгоритма шифрования, на диске. Ключ для этого симметричного алгоритма формируется либо из пароля пользователя для регистрации в системе, либо из ключа, хранящегося на смарт-карте, если регистрация при помощи смарт-карты разрешена.

Таким образом, система EFS может расшифровать закрытый ключ во время регистрации пользователя в системе и хранить его в своем виртуальном адресном пространстве во время работы, чтобы иметь возможность расшифровывать 128-разрядные ключи файлов без дополнительного обращения к диску. Когда компьютер выключается, закрытый ключ стирается из виртуального адресного пространства системы EFS, так что никто, даже украв компьютер, не получит доступа к закрытому ключу.

Потенциальная потребность в совместном использовании зашифрованных файлов является одной из причин, по которой применяется такая двухуровневая система ключей. Если бы все файлы зашифровывались ключами владельцев файлов, то совместное использование зашифрованных файлов было бы невозможным. Эта проблема может быть решена, если для зашифровки каждого файла использовать отдельный ключ.

Схема с использованием случайных ключей для шифрования файлов, но с шифрованием самих ключей при помощи симметричного алгоритма шифрования не будет работать. Проблема в том, что наличие симметричного ключа, хранящегося на диске в открытом виде, разрушит всю систему защиты - сформировать ключ дешифрации по ключу шифрования слишком легко. Таким образом, медленное шифрование с открытым ключом требуется для шифрования ключей файлов.

Поскольку ключи шифрования все равно являются открытыми, хранение их в открытом виде не представляет опасности.

Вторая причина использования двухуровневой системы ключей заключается в производительности. Использование криптографии с открытым ключом для шифрования файлов было бы слишком медленным. Для повышения эффективности шифрование с открытым ключом применяется лишь для зашифровки коротких 128-разрядных ключей файлов, тогда как для шифрования самих файлов используется симметричный алгоритм.

2.3 *Агенты восстановления данных*

Ключи шифрования закреплены за учетной записью пользователя, и при ее удалении или потере ключей шифрования зашифрованные с их помощью файлы расшифровать практически невозможно. Для того, чтобы избежать потери зашифрованных данных и создаются агенты восстановления.

Агент восстановления данных - это пользователь, наделенный полномочиями для расшифровки данных, зашифрованных другими пользователями с помощью стандартных средств шифрования Windows**.** Обычно правами агентов восстановления наделяются администраторы, но это может быть и любой другой пользователь.

Процедура создания агента восстановления данных:

1. **Войти в систему под учетной записью пользователя, который будет выполнять роль агента восстановления.** Пользователь долен иметь права администратора или входить в группу **«Криптографические**

операторы»

2. **Создать сертификаты ключей шифрования для агента восстановления данных.**

   Для этих целей используется консольная утилита **Cipher.**

- *Открыть командную строку.*

  Пуск => Все программы *=>* ***Стандартные*** *=>* ***Командная строка*** *(или набрать команду* ***cmd*** *в поле ввода* ***Найти программы и файлы*** *в меню* ***Пуск*** *).*

- *В открывшемся окне ввести команду* ***Cipher /R:key_name,*** *где* ***key_name*** *- название для файлов ключей, которые будут созданы****.***

- *После ввода команды будет предложено задать пароль для сертификата закрытого ключа, а затем повторить его. Этот пароль следует запомнить или записать, поскольку он понадобится при дальнейшем использовании ключа, в том числе и при его импорте в хранилище.*

- *После ввода пароля будут созданы два файла* ***key_name.cer*** *- с открытым ключом и* ***key_name.pfx*** *-_ с закрытым ключом шифрования. По умолчанию эти файлы сохраняются в папку пользователя, но при желании можно задать и другой путь, задав его с помощью команды* ***cd*** *перед использованием Cipher.*

3. **Импортировать закрытый ключ *key_name.pfx* в хранилище личных сертификатов**

- *Для импорта закрытого ключа дважды щелкнуть мышью файл ключа, откроется диалоговое окно* ***Мастер импорта сертификатов***

- *В открывшемся диалоговом окне мастера нажать кнопку* ***Далее*** *для перехода к следующему шагу. Если путь к сертификату не отображается в поле ввода* ***Имя файла****. Нажать кнопку* ***Обзор*** *и в диалоговом окне выбора файла указать путь к файлу закрытого ключа. Нажать кнопку* ***Далее.***

- *В поле ввода текста* ***Пароль*** *ввести пароль к закрытому ключу, который указали при его создании. Если пароль указан неверно, система выведет соответствующее предупреждение. Установить флажок* ***Включить все расширенные свойства****. Остальные флажки следует снять. Затем нажать кнопку* ***Далее.***

- *Выбрать хранилище сертификатов. Установить переключатель в положение* ***Поместить все сертификаты в следующее хранилище,***

*затем нажать кнопку **Обзор** и в открывшемся диалоговом окне выбрать **Личное**.*

- *Нажать кнопку **Далее**, а затем **Готово**. При успешном импорте система выведет соответствующее сообщение.*

4. Внести открытый ключ *key_name.cer* в список сертификатов пользователей - агентов восстановления данных.

- *Войти в систему под учётной записью администратора*
- *Открыть узел **Политика «Локальный компьютер» \ «Конфигурация компьютера \ Конфигурация Windows \ Параметры безопасности \ Политики открытого ключа***
- *Щелкнуть правой кнопкой мыши по контейнеру **Шифрующая файловая система EFS** и выбрать в контекстном меню команду **Добавить агент восстановления данных**. Откроется диалоговое окно **Мастер добавления агента восстановления**.*
- *В открывшемся диалоговом окне нажать кнопку **Далее** для перехода к следующему шагу.*
- *Нажать кнопку **Обзор папок** и с помощью открывшегося диалогового окна выбрать созданный на предыдущем этапе файл **key_name.cer.***
- *Данные о пользователе, которому принадлежит ключ, отобразятся в списке диалогового окна мастера. Повторить шаг 4, если требуется добавить несколько пользователей в качестве агентов восстановления данных. Затем нажать кнопку **Далее** для перехода к последнему шагу мастера и нажать кнопку **Готово**. Добавленные ключи, сроки и область их действия, а также данные об их владельцах отобразятся в контейнере **Шифрующая файловая система EFS** (Encrypting File System).*

Добавление агента восстановления для средства шифрования диска **BitLocker** осуществляется тем же способом, что и для шифрующей файловой системы (в Windows 7 шифрование дисков с помощью **BitLocker** поддерживается в изданиях «Максимальная» и «Корпоративная»).

Для расшифровки зашифрованных другими пользователями данных пользователь, наделенный правами агента восстановления, использует свой закрытый ключ шифрования.

После импорта закрытого ключа пользователь, наделенный правами агента восстановления данных, сможет просматривать зашифрованные другими пользователями файлы так, как будто они зашифрованы им самим. Проверить наличие полномочий пользователя и, соответственно, правильности настройки политики можно в свойствах любого зашифрованного файла.

Для просмотра пользователей, наделенных правами агентов восстановления:

1. *Щелкнуть правой кнопкой мыши по зашифрованному файлу (обычно зашифрованные файлы выделены зеленым цветом) и выбрать команду* ***Свойства****.*

2. *На вкладке* ***Общие*** *диалогового окна свойств файла нажать кнопку* ***Другие*** *и в открывшемся диалоговом окне нажать кнопку* ***Подробно*** *. Откроется диалоговое окно* ***Пользовательский доступ к файлу****.*

3. *В нижней части окна в списке* ***Сертификаты восстановления для этого файла, определенные в политике восстановления*** *должны отображаться сертификаты пользователей, наделенных полномочиями агентов восстановления.*

Т.к. описываемые политики располагаются в узле **Конфигурация компьютера**, правами агента восстановления пользователя можно наделить только на данном компьютере, для других компьютеров сети процедуру создания агента восстановления данных следует повторить.

2.4 *Политики паролей учетных записей*

Параметры, предназначены для установки различных политик, связанных с паролями для входа в систему Windows, расположены в узле

Политика «Локальный компьютер» \ Конфигурация компьютера \ Конфигурация Windows \ Параметры безопасности \ Политики учетных записей

Использование данных политик позволяет усложнить несанкционированный доступ к компьютеру.

2.4.1 Ведение журнала паролей

Настройка **Вести журнал паролей** определяет число новых уникальных паролей, которые назначаются пользователем до установки ранее

использовавшегося пароля. Пользователь периодически может менять пароль для входа в систему. При этом он может использовать как новые пароли, так и ранее установленные. С помощью данной настройки устанавливается количество уникальных паролей (не использовавшихся ранее). Использовав установленное количество новых паролей, пользователь сможет задать ранее использовавшийся пароль.

Чтобы задать количество уникальных паролей, необходимо выполнить следующие действия.

1. Открыть узел ***Политика «Локальный компьютер» \ Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\ Политики учетных записей\ Политика паролей****.*

2. Дважды щелкнуть мышью по параметру ***Вести журнал паролей****. Появится диалоговое окно с единственным полем ввода.*

По умолчанию в поле ***Вести журнал для*** *указано значение 0 (ноль). Это означает, что журнал паролей не ведется, и пользователь может два и более раз подряд устанавливать один и тот же пароль для входа в систему. Увеличив это значение, например, до трех, можно задать количество уникальных паролей, которые нужно будет установить, прежде чем можно вернуться к ранее использовавшемуся паролю.*

3. В поле ***Вести журнал для*** *ввести нужное количество паролей, которые будут храниться в журнале.*

4. Нажать кнопку ОК, чтобы применить изменения и закрыть диалоговое окно.

Теперь, если, указанное количество уникальных паролей, попытаться задать ранее использовавшийся пароль, на экране появится сообщение о том, что указанный пароль не соответствует установленным требованиям политики паролей.

Закрыв появившееся сообщение, можно указать новый пароль. Если пароль будет уникальным или ранее уже использовали заданное количество уникальных паролей, данное сообщение не появится, и можно установить желаемый пароль для входа в систему.

Изменения вступают в силу без перезагрузки компьютера.

2.4.2 Максимальный срок действия пароля

Параметр **Максимальный срок действия пароля** определяет, какое количество дней будет действовать пароль, установленный на вход в систему до момента, когда пользователю будет предложено изменить пароль.

Диалоговое окно настройки **Максимальный срок действия пароля** вызывается щелчком по одноименному пункту в узле **Политика паролей**.

Данное диалоговое окно содержит единственное поле со счетчиком. По умолчанию в данном поле установлено значение 0 (ноль). Это означает, что срок действия пароля неограничен. В данном поле вы можете указать нужный вам срок действия пароля (в днях). Максимальный срок действия пароля — 999 дней.

По истечении указанного периода при загрузке Windows будет предложено изменить пароль. Можно указать новый пароль или ввести тот же самый (если в настройке **Вести журнал паролей** указано значение 0 (ноль)).

2.4.3 Минимальный срок действия пароля

Настройка **Минимальный срок действия пароля** определяет срок, в течение которого пользователь должен использовать текущий пароль, прежде чем изменить его. Например, если установить минимальный срок действия пароля сроком на 7 дней, пользователь не сможет изменить пароль ранее, чем через семь дней.

Диалоговое окно данной настройки вызывается при двойном щелчке мышью по настройке **Минимальный срок действия пароля**, расположенной в узле **Политика паролей**.

В поле со счетчиком указывается минимальный срок действия пароля (в днях) от 1 до 998. Если в данном поле указать значение 0 (ноль), пользователь может изменять пароль в любое время без каких-либо ограничений.

Если пользователь попытается сменить пароль ранее указанного минимального срока (отсчет ведется от последней смены пароля), на экране появится сообщение о том, что указанный пароль не соответствует установленным требованиям политики паролей.

2.4.4 Минимальная длина пароля

С помощью этой настройки задается минимальное количество знаков (букв или цифр), из которых может состоять пароль. Чем длиннее пароль, тем сложнее его подобрать с целью несанкционированного доступа к компьютеру.

Диалоговое окно данной настройки вызывается двойным щелчком мыши по настройке **Минимальная длина пароля**, расположенной в узле **Политика паролей**.

Окно настройки содержит одно поле со счетчиком, в котором указывается минимально допустимая длина пароля. Если вы установите минимальную длину пароля, а затем попытаетесь указать новый пароль, длина которого ниже минимально допустимой, на экране появится сообщение о том, что указанный пароль не соответствует установленным требованиям политики паролей.

Минимальная длина пароля может составлять от 0 до 14 символов.

2.4.5 Требования сложности пароля

Настройка **Пароль должен отвечать требованиям сложности**, расположенная в узле **Политика паролей**, позволяет исключить возможность ввода простых паролей.

Многие пользователи создают пароли, совпадающие с именем учетной записи либо состоящие из одинаковых символов, например 11111. Злоумышленники в первую очередь пытаются подобрать пароль, используя подобные комбинации, а значит, такие пароли небезопасны.

При включении настройки **Пароль должен отвечать требованиям сложности** (Password must meet complexity requirements) пользователь не сможет создать пароль, если он не отвечает следующим требованиям:

- длина пароля должна составлять не менее шести символов;
- пароль не содержит имени учетной записи либо частей имени;
- содержать знаки трех из четырех категорий: латинские прописные буквы (A-Z), латинские строчные буквы (a-z), цифры (0-9), отличающиеся от букв и цифр знаки, например %, #, $.

Например, пароль **ABsa95** отвечает требованиям безопасности, поскольку он не совпадает с именем учетной записи, состоит не менее чем из шести символов, а также содержит и прописные, и строчные буквы, и цифры, то есть знаки из трех ранее указанных категорий.

Диалоговое окно настройки **Пароль должен отвечать требованиям сложности** содержит всего один переключатель, с помощью которого можно включить либо отключить данную настройку. Если настройка включена, то при попытке создать пароль, не отвечающий требованиям сложности, на экране появится сообщение о том, что указанный пароль не соответствует установленным требованиям политики паролей.

2.4.6 Хранение паролей с использованием обратимого шифрования

Данная настройка определяет, будет ли использоваться метод обратимого шифрования для хранения паролей. Эта политика обеспечивает поддержку приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности.

Хранение паролей, использующих обратимое шифрование, не является безопасным, поэтому включение данной политики целесообразно только тогда, когда требования приложения не станут более весомыми, чем требования по защите паролей.

2.5 *Политика блокировки учетных записей*

В узле **Политика блокировки учетных записей** содержатся настройки, с помощью которых задаются параметры блокировки учетных записей.

2.5.1 Пороговое значение блокировки

Настройка **Пороговое значение блокировки** определяет количество неудачных попыток ввода пароля до блокировки системы.

Диалоговое окно данной настройки вызывается при двойном щелчке мышью по настройке **Пороговое значение блокировки**, расположенной в узле **Политика блокировки учетных записей**.

В диалоговом окне настройки **Пороговое значение блокировки** содержится всего одно поле со счетчиком. В данном поле указывается

количество попыток неудачного ввода пароля, которое будет приводить к блокировке учетной записи.

Количество попыток ввода пароля может составлять от 0 до 999. При установке значения 0 (ноль) учетная запись не будет блокироваться вне зависимости от того, сколько раз был введен неправильный пароль.

Количество попыток ввода неверного пароля будет ограничено. После того, как попытки ввода неверного пароля будут исчерпаны, учетная запись будет заблокирована. Разблокировка учетной записи может быть осуществлена администратором, либо разблокировка произойдет автоматически через заданное время.

Блокировка учетной записи существенно усложняет процесс подбора пароля.

2.5.2 Продолжительность блокировки учетной записи

Изменение данной настройки возможно, если в настройке **Пороговое значение блокировки**, описанной выше, установлено значение, отличное от нуля, то есть режим блокировки учетной записи включен.

Настройка **Продолжительность блокировки учетной записи** определяет интервал времени, в течение которого учетная запись будет заблокирована в случае ввода неверного пароля заданное количество раз.

Продолжительность блокировки может составлять от нуля до 99999 минут. Если вы установите значение 0 (ноль), учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную.

При блокировке учетной записи в окне приветствия Windows появляется сообщение о том, что учетная запись заблокирована и не может быть использована для входа в сеть. Следующие попытки входа в систему будут возможны по истечении указанного интервала блокировки.

2.5.3 Время до сброса счетчика блокировки

Настройка **Время до сброса счетчика блокировки** определяет интервал времени, через который будет осуществлен сброс счетчика блокировки после неудачной попытки ввода пароля. Допустим, у нас установлена блокировка

учетной записи после трех неудачных попыток ввода пароля. И время до сброса счетчика блокировки установлено равным пяти минутам. Мы ввели неверный пароль (у нас осталось две попытки), но повторно пытаться не стали. По прошествии пяти минут счетчик блокировки сбрасывается, и снова есть три попытки.

Интервал времени до сброса счетчика блокировки может быть назначен от 1 до 99999 минут.

2.6 *Политики аудита*

Политики аудита расположены в узле

Политика «Локальный компьютер» \ Конфигурация компьютера \ Конфигурация Windows \ Параметры безопасности \ Локальные политики \ Политики аудита

В данном узле содержится несколько настроек, и каждая из них определяет, будет ли фиксироваться в системе то или иное событие. Тип события как раз и определяется конкретной настройкой. Все настройки в данном узле содержат одинаковые диалоговые окна, в которых присутствуют два флажка: **Успех** и **Отказ**.

Если установлен флажок **Успех**, будет фиксироваться успешное, то есть выполненное событие.

Если же установить флажок **Отказ**, то фиксироваться будет так же незаконченное, то есть невыполненное событие, но при условии, что пользователь пытался выполнить это событие.

Например, если установить флажок **Успех** в диалоговом окне настройки **Аудит входа в систему**, система будет фиксировать (администратор сможет просмотреть эти события) успешные входы и выходы пользователей в Windows. Неудачные попытки входа (например, в случае неправильно набранного пароля) фиксироваться не будут.

Однако, если установить флажок **Отказ**, фиксироваться будут в том числе и неудачные попытки входа в систему.

Настройки, доступные в узле **Политика аудита**:

1. Аудит входа в систему. Аудиту подвергается успешный или не успешный вход в операционную систему, а также выход из нее;

2. **Аудит доступа к объектам**. Данная настройка выполняет аудит доступа к объектам, не относящимся к Active Directory. В качестве объектов могут выступать файлы, папки, принтеры, разделы системного реестра:

3. **Аудит доступа к службе каталогов**. Настройка выполняет аудит доступа к объектам, относящимся к Active Directory, для которых указан список управления доступом;

4. **Аудит изменения политики**. Данная настройка ведет аудит изменения политик пользователем;

5. Аудит изменений привилегий. Даная настройка определяет, будет ли выполняться аудит попыток изменения политики назначения прав пользователям;

6. **Аудит отслеживания процессов**. Выполняет аудит событий, связанных с процессами, например, создания или завершения процесса, а также обработке дублирований и непрямого доступа к объектам;

7. **Аудит системных событий**. Выполняет аудит системных событий. К системным событиям можно отнести изменение системного времени, запуск и отключение системы безопасности, загрузку компонентов расширяемой проверки подлинности, потерю отслеживаемых событий, а также превышение размера журнала установленного уровня.

8. **Аудит событий входа в систему**. Эта настройка определяет, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учетных данных. При использовании этой политики создается событие для локального и удаленного входа пользователя в систему;

9. **Аудит управления учетными записями**. Данная политика определяет, будут ли создаваться события при управлении учетными записями в системе и, соответственно, будет ли выполняться аудит этих событий.

2.7 *Назначение прав пользователя=>*

В узле

Политика «Локальный компьютер»\ Конфигурация компьютера\ Конфигурация Windows \Параметры безопасности\Локальные политики\Назначение прав пользователя

сосредоточено более сорока политик, с помощью которых можно задать или ограничить права пользователя.

Можно разрешить или запретить выполнять определенные действия для категорий пользователей или конкретных пользователей.

Все настройки имеют одинаковые диалоговые окна, в которых приводится список категорий пользователей. Чтобы разрешить выполнять выбранное действие, нужно добавить в список или категорию пользователей, или конкретного пользователя.

Например, настройка **Создание файла подкачки** определяет пользователей, которым разрешено создавать файлы подкачки. По умолчанию данное действие позволено выполнять только администраторам.

Чтобы добавить категорию пользователей, которым разрешено создавать файлы подкачки, нужно выполнить следующие действия:

*1. В диалоговом окне настройки данной политики нажать кнопку **Добавить пользователя или группу**. На экране появится диалоговое окно выбора пользователей или групп.*

2. С помощью появившегося диалогового окна надо найти пользователей или группы, которых необходимо добавить в список разрешений.

3. Нажать кнопку ОК, чтобы закрыть диалоговое окно выбора пользователей или групп.

4. Убедиться, что выбранные вами пользователи или группы появились в списке диалогового окна настройки политики.

5. Нажать кнопку ОК, чтобы закрыть диалоговое окно.

Группы пользователей можно выбрать, нажав кнопку **Типы объектов** в диалоговом окне выбора пользователей или групп. При нажатии данной кнопки появляется диалоговое окно со списком типов объектов. Для тех типов, которые

необходимо выбрать, следует установить флажки. Также можно добавить конкретных пользователей, выполнив их поиск на локальном и сетевых компьютерах.

С помощью кнопки **Размещение** выбирается размещение пользователя (имя компьютера в сети или рабочая группа, в которой следует выполнить поиск имен).

С помощью кнопки **Проверить имена** выполняется проверка имен, указанных в поле слева. Проверка имен выполняется в размещении, указанном вами с помощью диалогового окна, появляющегося при нажатии кнопки **Размещение** (Locations).

Некоторые из Политики, расположенные в рассматриваемом узле:

- **Блокировать страницы в памяти**. Эта политика определяет пользователей и группы, которые могут использовать процессы для сохранения данных в физической памяти для предотвращения сброса этих данных в виртуальную память на диске. Блокировка страниц в памяти уменьшает свободный объем ОЗУ, что сказывается на снижении быстродействия системы;
- **Загрузка** и **выгрузка драйверов устройств** . С помощью данной политики можно назначить права на динамическую загрузку или выгрузку драйверов устройств. По умолчанию такую привилегию имеет только администратор. Политика не распространяется на драйверы устройств Plug and Play;
- **Замена маркера уровня процесса**. Эта политика позволяет определить учетные записи, которым позволено вызывать процедуру API-интерфейса
- **CreateProcessAsUser( )** Данный интерфейс позволяет одной службе запускать другую;
- **Изменение метки объекта**. Эта политика определяет пользователей, которым разрешено изменять метки целостности объектов, владельцами которых являются другие пользователи.

Примеры объектов - файлы, разделы реестра или процессы;

- **Настройка квот памяти для процесса**. Здесь можно назначить пользователей и группы, которым разрешено изменять максимальный объем памяти, используемый процессом. По умолчанию разрешение выдано администраторам, а также локальным и сетевым службам;
- **Смена владельцев файлов и других объектов**. Политика позволяет назначить пользователей, которые могут стать владельцами любого защищенного объекта в системе. Например, вы можете назначить пользователя, который будет иметь право изменять собственника файла или папки. По умолчанию разрешение дано администраторам;
- **Создание аудитов безопасности**. Политика определяет субъекты, которые будут использоваться процессом для добавления в журнал безопасности. По умолчанию разрешение выдано локальной и сетевой службе;
- **Создание файла подкачки**. Дает право на управление (создание, изменение и удаление) файлом подкачки Windows. По умолчанию разрешение дано администраторам;
- **Увеличение приоритета выполнения**. Политика определяет пользователей, которым разрешено использовать процесс, дающий право на повышение приоритета выполнения другого процесса;
- **Увеличение рабочего набора процессов**. Дает право на уменьшение или увеличение размера рабочего набора процесса, то есть набора страниц памяти, видимых процессу в физической оперативной памяти:
- **Управление аудитом и журналом безопасности**. Данная политика определяет пользователей, которые могут управлять политиками аудита. По умолчанию разрешение выдано администраторам.

2.8 *Параметры безопасности данных и функционирования системы*

В узле

Политика «Локальный компьютер» \ Конфигурация компьютера \ Конфигурация Windows \ Параметры безопасности \ Локальные политики \ Параметры безопасности

сосредоточено большое количество различных политик, отвечающих за безопасность данных и работы на компьютере. Диалоговые окна настройки политик достаточно просты, и в большинстве своём содержат единственный элемент управления: переключатель, раскрывающийся список, поле ввода или поле со счетчиком.

Некоторые из политик, расположенные в узле Параметры безопасности (Security Options):

- **Аудит: аудит доступа глобальных системных объектов**. С помощью данной политики включается или отключается аудит доступа к глобальным системным объектам — мьютексам, семафорам и так далее;
- **Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности**. Если включить данную политику, то в случае невозможности системы внести запись о событии, подлежащем аудиту, происходит отключение системы. Одна из причин невозможности протоколирования событий — переполнение журнала аудита безопасности;
- **Завершение работы: очистка файла подкачки виртуальной памяти.** Если данная политика включена, при завершении работы системы автоматически будет выполняться очистка файла подкачки виртуальной памяти;
- **Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему**. Данная политика используется только если в политике **Интерактивный вход в систему: текст сообщения для пользователей при входе** в **систему** указан какой-либо текст. Эта

политика задает текст заголовка для сообщения, которое выводится в окне входа в Windows;

- **Интерактивный вход в систему: напоминать пользователю об истечении срока действия пароля**. С помощью данной политики можно установить, за сколько дней до истечения срока действия пароля пользователь будет получать напоминание об окончании срока действия пароля. Напоминание происходит при входе пользователя в систему;
- **Интерактивный вход в систему: не отображать последнее имя пользователя**. Данная политика позволяет включить или отключить режим отображение в окне входа в Windows имени последнего пользователя, выполнившего вход в систему;
- **Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL**. По умолчанию поведение политики не определено, и нажатия указанного сочетания клавиш для входа в систему не требуется. Однако можно включить запрос на нажатие сочетания клавиш **Ctrl+Alt+Del** для входа в систему;
- **Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован**. С помощью данной политики можно задать тип сведений, которые будут отображаться на экране при заблокированном сеансе. На экране может отображаться выводимое имя пользователя, а также имена домена и пользователя, либо только имя пользователя. Также можно отключить вывод каких-либо сведений о пользователе;
- **Интерактивный вход в систему: текст сообщения для пользователей при входе в систему**. С помощью данной политики можно указать текст, который будет выводиться на экране входа в Windows. Данный текст может содержать, например, какие-либо предупреждения или указания для всех пользователей, пытающихся войти в систему;
- **Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в размещение пользователя**. Данный параметр служит для уменьшения опасности программ. По умолчанию он включен, и если

программа, не имеющая прав на запись данных в папку Program Files Windows или в ветвь реестра HKLM\ Software\, пытается выполнить такую операцию, то эти данные будут перенаправлены в пользовательскую область. Если параметр отключить, то такая операция будет завершаться ошибкой;

- **Системная криптография: использовать FIPS 140-совместимые алгоритмы для шифрования, хеширования и подписывания**. При включении данного параметра в операционной системе для криптографических операций будут использоваться только протоколы, соответствующие стандарту FIPS 140;
- **Системная криптография: применять сильную защиту пользовательских ключей, хранящихся на компьютере**. Параметр определяет необходимость ввода пользователем пароля при работе с закрытым ключом шифрования. В зависимости от выбранного значения пароль не будет требоваться, будет запрашиваться при первом или при каждом обращении к закрытому ключу;
- **Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям**. Определяется доступ для дисководов оптических дисков:
- **Устройства: разрешить форматирование и извлечение съемных носителей**. Данная политика определяет группы пользователей, которые могут форматировать и извлекать NTFS-носители. Возможные варианты: Администраторы, Администраторы и опытные пользователи, Администраторы и интерактивные пользователи;
- **Учетные записи: переименование учетной записи администратора** . С помощью данной политики можно изменить имя учетной записи администратора (по умолчанию - Администратор);
- **Учетные записи: переименование учетной записи гостя** (Accounts Rename guest account). Данная политика позволяет изменить имя учетной записи гостя. По умолчанию — **Гость**

- **Учетные записи: ограничить использование пустых паролей только консольным входом**. С помощью данной политики можно запретить или разрешить использование пустых паролей при удаленном подключении к системе. Если параметр включен, то использовать учетную запись без пароля для входа в систему можно только с самого компьютера;
- **Учетные записи: состояние учетной записи «Администратор»**. С помощью этой политики можно включить или отключить учетную запись локального администратора;
- **Учетные записи: состояние учетной записи «Гость».** Можно включить или отключить гостевую учетную запись.

3 Задание на выполнение работы

1. Войти в систему под учётной записью **StudXX, где XX -** индекс группы. Запустить виртуальную машину **Oracle VM VirtualBox**. Запустить гостевую операционную систему **Windows 7**.
2. Войти в гостевую операционную систему под учётной записью **StudXX, где XX -** индекс группы.
3. Создать на локальном диске С: папку **ДОКУМЕНТЫ**.
4. Установить для папки **ДОКУМЕНТЫ** атрибут ***Шифровать содержимое для защиты данных*****(**Контекстное меню – Свойства – Общие – Другие**)**
5. Войти в систему под учётной записью администратора **ИУ5**
6. Используя оснастку «Локальные пользователи и группы» создать пользователя с учётной записью **ИУ5_REC** и обычным доступом. Включить пользователя **ИУ5_REC** в группу **«Криптографические операторы»**
7. Выполнить процедуру назначения роли агента восстановления данных для пользователя **ИУ5_REC**.
8. Проверить правильность выполнения функций агентом восстановления данных.
9. Выполнить следующие настройки пароля для пользователя:

   - длина пароля должна быть не менее 5 символов;

- включите ведение журнала паролей, для того чтобы пользователь не мог заменить пароль на текущий.

10. Выполнить администрирование безопасности функционирования операционной системы используя узел

Политика «Локальный компьютер» \ Конфигурация компьютера \ Конфигурация Windows \ Параметры безопасности \ Локальные политики \ Параметры безопасности

4 Контрольные вопросы

1. Назовите назначение и основные функции системы безопасности ОС.
2. Назовите назначение открытого и закрытого ключей шифрования.
3. Что такое агент восстановления данных?
4. Для чего предназначены политики паролей учётных записей?
5. Для каких событий в системе может быть осуществлён аудит?
6. Назовите основные параметры безопасности данных и функционирования системы.

5 ЛИТЕРАТУРА

1. Матвеев М.Д., Прокди Р.Г. и др. Администрирование Windows 7. Практическое руководство и справочник администратора. – Спб.: Наука и техника, 2013.-400 стр.: ил.
2. Книттель Б., Windows 7. Скрипты, автоматизация и командная строка. –СПб.:Питер, 2012. – 784 с. : ил.