МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

Кафедра №51 «Безопасность информационных систем
На правах рукописи
Мошак Н.Н.

Учебно-методическое пособие к лабораторным работам

По курсу - Безопасность информационных систем

основная профессиональная образовательная программа:
09.04.02 – Информационные системы и технологии

Квалификация: бакалавр

Профиль **– Информационная безопасность**

Санкт-Петербург
2020

УДК 004.056

Мошак Н.Н. Безопасность информационных систем: учеб. метод. пособ. / ГУАП. – СПб, 2020.

Утверждено в качестве учебно-методического пособия редакционно-издательским советом университета.

Излагаются методические указания к лабораторным работам по курсу «Безопасность информационных систем», выполнение которых будет способствовать усвоению и закреплению пройденного теоретического курса. Пособие содержит задания к лабораторным работам, методические рекомендации по их выполнению и примеры. Практикум сопровождается кратким теоретическим материалом и справочной информацией. Структура практикумаотражает последовательность изложения материала в учебной программе и в учебном пособии Мошак Н.Н. Безопасность информационных систем: Учеб. пособие/ Н.Н. Мошак – СПб.: ГУАП, 2019. – 169 с. ISBN 978-5-8088-1414-1. Основное внимание в лабораторных работах уделяется техническим решениям по защите компьютерных ресурсов от несанкционированного доступа (НДС) на уровне рабочих станций раздела рабочей программы «Методы реализации основных требований политики информационной безопасности в элементах ИС».

Предназначено для подготовки бакалавров по профессиональной образовательной программе 10.04.01 Информационная безопасность. Профиль – Безопасность компьютерных систем.

Ответственный редактор – В.В. Овчинников.

Рецензенты – д-р.техн.наук., проф. В.А. Богатырев, д-р.техн.наук, проф. А.Н, Молдовян

Общие рекомендации по выполнениюлабораторных работ

1. **Методическиеуказания повыполнениюлабораторных работ**

Входевыполнениялабораторныхработобучающийсядолженуглубитьизакрепить знания,практическиенавыки,овладетьсовременнойметодикойитехникойэкспериментав соответствиисквалификационнойхарактеристикойобучающегося.Выполнение лабораторныхработсостоитизэкспериментально-практической,расчетно-аналитической частей и контрольных мероприятий.

Выполнениелабораторныхработобучающимсяявляетсянеотъемлемойчастью изучениядисциплины «Безопасность информационных систем»,определяемойучебнымпланомиотноситсяксредствам, обеспечивающимрешение следующихосновныхзадачуобучающегося:

- приобретениенавыковисследованияпроцессов,явленийиобъектов,изучаемых в рамкахданной дисциплины;
- закрепление, развитиеи детализация теоретическихзнаний,полученныхналекциях;
- получениеновой информации поизучаемой дисциплине;
- приобретениенавыковсамостоятельнойработыслабораторнымоборудованием и приборами.

2. **Заданияитребованияк проведениюлабораторных работ**

Вариантзаданияпокаждойлабораторнойработеобучающийсяполучаетв соответствиисномеромвспискегруппы.Передпроведениемлабораторнойработы обучающемусяследуетвнимательноознакомиться*сметодическимиуказаниям ипоее выполнению.*Всоответствиисзаданиемобучающийсядолженподготовитьнеобходимые данные,получитьотпреподавателядопускквыполнениюлабораторнойработы, выполнить указаннуюпоследовательностьдействий,получитьтребуемыерезультаты,оформитьи защитить отчет лабораторной работе.

3. **Оформление, структура и форма отчета по лабораторной работе**

Покаждойлабораторнойработевыполняетсяотдельныйотчет.Титульный лист оформляетсявсоответствиисшаблоном(образцом)приведеннымнасайтеГУАП (www.guap.ru)вразделе«Секторнормативнойдокументации».Текстовыеиграфические материалыоформляютсявсоответствиисдействующимиГОСТамиитребованиями, приведенныминасайтеГУАП(www.guap.ru)вразделе«Секторнормативной

документации».

Отчетполабораторнойработедолженвключатьвсебя:титульныйлист,формулировку задания,теоретическиеположения,используемыепривыполнениипрактической и/или лабораторнойработы, описаниепроцессавыполнения работы, полученныерезультаты и выводы.

ЛАБОРАТОРНАЯ РАБОТА № 1
НАСТРОЙКА ЛОКАЛЬНЫХ ПОЛИТИК БЕЗОПАСНОСТИ АРМ

1. Цель работы

Цель работы – изучить и научиться настраивать локальные политики безопасности на автономном автоматизированном рабочем месте (АРМ) пользователя с установленной на нем операционной системой (ОС)Windows для защиты информации от несанкционированного доступа (НСД).
Используемое программное обеспечение: ОС версии не ниже WindowsXP.

2. Задание к лабораторной работе

1. Сформулировать цель и задачу выполнения работы
2. Указать последовательностькоманд для выхода в диалоговые окна создания и удаления оснасток, а также настройки для каждой политики безопасности (4.2-4.7). Пример: Откроем «Политику паролей», перейдя по адресу: *Пуск → Выполнить → secpol.msc → Параметры безопасности → Политики учётных записей→ Политика паролей*
3. Объяснить критерии выбора политик безопасности (4.2-4.7) для защиты АРМ от НСД в «закрытом» и «открытом» контуре.
4. Обосновать настройки каждого параметра соответствующих локальных политик безопасности в «закрытом» и «открытом» контуре.
5. Привести скриншоты до и после настройки параметров соответствующих политик безопасности.

3. Краткие теоретические сведения

3.1. *Основные угрозы нарушения базовых услуг безопасности «конфиденциальность», «целостность» и «доступность» ресурсов АРМ*

Основные угрозы нарушения ***конфиденциальности*** ресурсов АРМ - этокомпрометация ключевой информации систем криптографической защиты информации и несанкционированноепредоставление привилегий пользователям в ОС Windows АРМ.

Основные угрозы нарушения ***целостности***программ и данных АРМ– это несанкционированное изменение операционной среды АРМ; действия нарушителя в среде ИС от имени легального пользователя, носящие деструктивный характер или приводящие к искажению информации.

Основные угрозы нарушения ***доступности***активов АРМ – изменения конфигурации ОС (файлов CONFIG.SYS и AUTOEXEC.BAT, файлов ядра ОС для Windows); удаления (модификации) исполняемых файлов

прикладного и системного программного обеспечения; внесения компьютерных вирусов; эксплуатации программ, осуществляющих некорректные действия, из-за имеющихся в них ошибок или специальных «закладок».

3.2. *Требования по защите АРМ от НСД «закрытого» и «открытого» контура ИС*

Подсистема защиты АРМ от НСД «закрытого» и «открытого» контура должна обеспечивать: однозначную идентификацию пользователей в ИС и в операционной системе (далее – ОС) АРМ (использование общих идентификаторов (ни в СЗИ, ни в ОС) не допускается; идентификацию по логическим именам информационных ресурсов (логических устройств, каталогов, файлов).

Управление доступом в АРМ должна базироваться на стандартных механизмах идентификации, аутентификации и разграничения доступа предоставляемых:

a) *BIOS ПЭВМ;*
b) *сертифицированным программно-аппаратным комплексом защиты от НСД СЗИ;*
c) *ОС Windows АРМ;*
d) *сетевой ОС;*
e) *СУБД;*
f) *средствами усиленной аутентификации ACE Server (SecurID) или Kerberos.*

Завершение работы пользователем АРМ должно сопровождаться освобождением всех занимаемых им разделяемых ресурсов (Logout).

Все входящие носители информации должны проверяться на наличие вирусов.

АРМ «закрытого» и «открытого» контура ИС должны защищаться от НСД с помощью сертифицированной системы защиты информации (СЗИ) от НСД. Настройка системы защиты от НСД на каждом АРМ осуществляется индивидуально, с учетом решаемых на этом АРМ задач, при этом, независимо от используемой операционной системы на АРМ, у пользователя не должно быть возможности запускать собственные, не разрешенные явно администратором безопасности, задачи.

В минимальной конфигурации СЗИ от НСД, устанавливаемые на АРМ пользователей, должны обеспечивать:

- создание изолированной (замкнутой) программной среды (ИПС) на АРМ, обеспечивающей возможность запуска только заданного набора программ и/или процессов. Создание ИПС на АРМ пользователя предполагает настройку СЗИ от НСД и/или средств реестра ОС Winows в режиме, обеспечивающем запуск только технологического программного обеспечения и запрет выполнения программ, не предусмотренных технологическим процессом. Управление ИПС АРМ должно осуществляться централизованно;

- идентификацию и аутентификацию пользователей, предоставление доступа к ресурсам компьютера только по предъявлению личного аппаратного идентификатора и дополнительным вводом пароля с клавиатуры;
- контроль ***целостности*** программных средств СЗИ от НСД до входа пользователя в операционную систему;
- разграничение доступа к локальным каталогам и файлам рабочей станции, обеспечивающее защиту от модификации системного и прикладного программного обеспечения АРМ;
- регистрацию попыток входа в систему и попыток доступа к важнейшим объектам локальной файловой системы компьютера;
- блокировку работы пользователей в случае нарушения ограничений, наложенных СЗИ от НСД.

Кроме того, настройка СЗИ от НСД должна запрещать пользователю выполнение следующих действий согласно приведенной табл. 3.1.

Таблица 3.1

Наименование запрета	Пояснения
Запрет загрузки с внешних носителей	Пользователю запрещается осуществлять загрузку компьютера с системной дискеты или с загрузочного CDROM диска
Запрет работы при нарушении целостности	При обнаружении факта нарушения целостности контролируемых файлов доступ пользователя к компьютеру блокируется.
Запрет работы при изъятии аппаратной поддержки	При обнаружении факта изъятия устройства аппаратной поддержки из компьютера доступ пользователя к компьютеру блокируется. При попытке пользователя войти в систему на экран будет выведено предупреждающее сообщение, и загрузка компьютера будет прервана
Запрет работы при изменении конфигурации	При обнаружении факта изменения конфигурации компьютера, доступ пользователя к компьютеру блокируется. При попытке пользователя войти в систему на экран выводится предупреждающее сообщение, и загрузка компьютера прерывается.
Запрет доступа к портам	Пользователю запрещается обмен информацией через коммуникационные порты компьютера.
Запрет на редактирование системного реестра	Пользователю запрещается изменять параметры системного реестра.
Запрет изменения настроек сети	Пользователю запрещено изменение параметров работы сетевой карточки, сетевых протоколов и других настроек «сетевого окружения» в

Наименование запрета	Пояснения
	операционной системе
Запрет изменения параметров безопасности	Пользователю запрещен доступ к изменению политик безопасности.
Запрет выполнения функций, не определенных технологическим процессом	Пользователю запрещено выполнять программное обеспечение, не используемое в технологическом процессе

Локальные политики безопасности АРМ – это набор параметров безопасности операционной системы Windows и системы защиты информации от НСД, которые обеспечивают безопасность АРМ в соответствии с требованиями политики информационной безопасности ИС организации. Для настройки локальной политики безопасности на автономном АРМ используется оснастка «Локальная политика безопасности». Если АРМ входит в состав домена, изменение политик,привязанных к домену ActiveDirectory, можно настраивать при помощи оснастки «Редактор управления групповыми политиками».

4. Последовательность выполненияработы

4.1. *Подготовка к настройкелокальных политик безопасности*

4.1.1. Установить макет варианта лабораторной работы на диске C (VirtualBox).

4.1.2. Перейти к настройке локальных политик безопасности, можно следующими способами:

a) Нажмите на кнопку «Пуск» для открытия меню, в поле поиска введите *Локальная политика безопасности* и откройте приложение в найденных результатах;

b) Воспользуйтесь комбинацией клавиш WIN+R для открытия диалога «Выполнить» (или вызывать диалог из меню кнопки «Пуск»). В диалоговом окне «Выполнить», в поле «Открыть» введите secpol.msc и нажмите на кнопку «ОК»;

c) Откройте «Консоль управления MMC». Для этого нажмите на кнопку «Пуск», в поле поиска введите mmc, а затем нажмите на кнопку «Enter». Откроется пустая консоль MMC. В меню «Консоль» выберите команду «Добавить или удалить оснастку» или воспользуйтесь комбинацией клавиш Ctrl+M. В диалоге «Добавление и удаление оснасток» выберите оснастку «Редактор локальной групповой политики» и нажмите на кнопку «Добавить». В появившемся диалоге «Выбор объекта групповой политики» нажмите на кнопку «Обзор» для выбора компьютера или нажмите на кнопку «Готово» (по умолчанию установлен объект «Локальный компьютер»). В диалоге «Добавление или удаление оснасток» нажмите на кнопку «ОК».

Для успешного выполнения настроек политик, учетная запись, под которой выполняются данные действия, должна входить в локальную группу «Администраторы» на локальном компьютере. Если компьютер подключен к домену, то эти действия могут выполнять только пользователи, которые являются членами группы «Администраторы домена» или групп, с разрешенными правами на редактирование политик.

4.2. ***Управление встроенными учетными записями***

Встроенными учетными записями являются учетные записи гостя и администратора. В этом примере мы переименуем гостевую учетную запись. Для этого выполните следующие действия:

a) Откройте оснастку *«Локальные политики безопасности»**;***
b) Перейдите в узел «Локальные политики», а затем «Параметры безопасности»;
c) Откройте параметр «Учетные записи: Переименование учетной записи гостя» дважды щелкнув на нем или нажав на клавишу Enter;
d) В текстовом поле введите *Гостевая запись* и нажмите на кнопку «ОК»;
e) Перезагрузите компьютер.

После перезагрузки компьютера для того чтобы проверить, применилась ли политика безопасности к вашему компьютеру, вам нужно открыть в панели управления компонент «Учетные записи пользователей» и перейти по ссылке «Управление другой учетной записью». В открывшемся окне вы увидите все учетные записи, созданные на вашем локальном компьютере, в том числе переименованную учетную запись гостя.

Также можно изменять состояния встроенных учетных записей через параметры *«Учетные записи: Состояние учетной записи «Гость» и «Учетные записи: Состояние учетной записи «Администратор», устанавливая значения «Включен» или «Выключен». По умолчанию гостевая учетная запись выключена. Учетную запись администратора выключать не рекомендуется! Однако хорошей практикой читается переименование встроенной учетной записи администратора.*

4.3. ***Управление политиками паролей***

a) Откройте оснастку «Локальные политики безопасности»;
b) Перейдите в узел «Политики учетных записей» и откройте параметр «Политики паролей».

Вы можете использовать до шести политик безопасности, при помощи которых можно указать наиболее важные параметры безопасности, применяемые для управления паролями учетных записей. Настоятельно рекомендуется не игнорировать данные политики. Даже если вы уговорите пользователей использовать сложные пароли, не факт, что они действительно будут это делать. Если вы правильно настроите все шесть политик безопасности, расположенных в этом узле, безопасность паролей пользователей вашей организации значительно повысится. Применив все политики, пользователям действительно придется создавать безопасные

пароли, в отличие от тех, которые они считают «сложными». Список политик:

Максимальные срок действия пароля. Эта политика указывает период времени, в течение которого пользователь может использовать свой пароль до последующего изменения. По окончанию установленного срока пользователь обязан изменить свой пароль, так как без изменения пароля войти в систему ему не удастся. Доступные значения могут быть установлены в промежутке от 0 до 999 дней. Если установлено значения равное 0, срок действия пароля неограничен. В связи с мерами безопасности желательно отказаться от такого выбора. Если значения максимального срока действия пароля варьируется от 1 до 999 дней, значение минимального срока должно быть меньше максимального. Лучше всего использовать значения от 30 до 45 дней.

Минимальная длина пароля. При помощи этой политики вы можете указать минимальное количество знаков, которое должно содержаться в пароле. Если активировать этот параметр, то при вводе нового пароля количество знаков будет сравниваться с тем, которое установлено в этой политике. Если количество знаков будет меньше указанного, то придется изменить пароль в соответствии с политикой безопасности. Можно указать значение политики от 1 до 14 знаков. Оптимальным значением для количества знаков для пароля пользователей является 8, а для серверов от 10 до 12.

Минимальные срок действия пароля. Многие пользователи не захотят утруждать себя запоминанием нового сложного пароля и могут попробовать сразу при вводе изменить такое количество новых паролей, чтобы использовать свой хорошо известный первоначальный пароль. Для предотвращения подобных действий была разработана текущая политика безопасности. Вы можете указать минимальное количество дней, в течение которого пользователь должен использовать свой новый пароль. Доступные значения этой политики устанавливаются в промежутке от 0 до 998 дней. Установив значение равное 0 дней, пользователь сможет изменить пароль сразу после создания нового. Необходимо обратить внимание на то, что минимальный срок действия нового пароля не должен превышать значение максимального срока действия.

Пароль должен отвечать требованиям сложности. Это одна из самых важных политик паролей, которая отвечает за то, должен ли пароль соответствовать требованиям сложности при создании или изменении пароля. В связи с этими требованиями, пароли должны:

a) содержать буквы верхнего и нижнего регистра одновременно;
b) содержать цифры от 0 до 9;
c) содержать символы, которые отличаются от букв и цифр (например, !, @, #, $, *);
d) Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

Требованиенеповторяемости паролей. Указывается количество предыдущих паролей пользователя, с которыми будет сравниваться новый пароль.

*Хранение паролей, используя обратимое шифрование.*Для того чтобы пароли невозможно было перехватить при помощи приложений, ActiveDirectory хранит только хэш-код. Но если перед вами встанет необходимость поддержки приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности, вы можете использовать текущую политику. Обратимое шифрование по умолчанию отключено, так как, используя эту политику, уровень безопасности паролей и всего домена в частности значительно понижается. Использование этой функции аналогично хранению пароля в открытом виде.

4.4. ***Политика блокировки учетной записи***

a) Откройте оснастку *«Локальные политики безопасности»**;***
b) Перейдите в узел «Политики учетных записей» и откройте параметр «Политика блокировки учетных записей».

Даже после создания сложного пароля и правильной настройки политик безопасности, учетные записи ваших пользователей все еще могут быть подвергнуты атакам недоброжелателей. Например, если вы установили минимальный срок действия пароля в 20 дней, у хакера достаточно времени для подбора пароля к учетной записи. Узнать имя учетной записи не является проблемой для хакеров, так как, зачастую имена учетных записей пользователей совпадает с именем адреса почтового ящика. А если будет известно имя, то для подбора пароля понадобится какие-то две-три недели.

Политики безопасности Windows могут противостоять таким действиям, используя набор политик узла *«Политика блокировки учетной записи»*. При помощи данного набора политик, у вас есть возможность ограничения количества некорректных попыток входа пользователя в систему. Разумеется, для ваших пользователей это может быть проблемой, так как не у всех получится ввести пароль за указанное количество попыток, но зато безопасность учетных записей перейдет на «новый уровень». Для этого узла доступны только три политики:

Установить время до сброса счетчиков блокировки. ActiveDirectory и групповые политики позволяют автоматически разблокировать учетную запись, количество попыток входа в которую превышает установленное вами пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Вы можете установить значение от одной минуты до 99999. Это значение должно быть меньше значения политики *«Продолжительность блокировки учетной записи»*.

Установить пороговое значение блокировки. Используя эту политику, вы можете указать количество некорректных попыток входа, после чего учетная запись будет заблокирована. Окончание периода блокировки учетной записи задается политикой *«Продолжительность блокировки*

учетной записи» или администратор может разблокировать учетную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. Я рекомендую устанавливать допустимое количество от трех до семи попыток.

Установить продолжительность блокировки учетной записи. При помощи этого параметра вы можете указать время, в течение которого учетная запись будет заблокирована до ее автоматической разблокировки. Вы можете установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0, учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную.

4.5. ***Политика аудита***

a) Откройте оснастку *«Локальные политики безопасности»**;***
b) Перейдите в узел «Локальные политики» и откройте параметр «Политика аудита».

После того как политики безопасности учетных записей у вас правильно настроены, злоумышленникам будет намного сложнее получить доступ к пользовательским учетным записям. Но не стоит забывать о том, что на этом ваша работа по обеспечению безопасности сетевой инфраструктуры не заканчивается. Все попытки вторжения и неудачную аутентификацию ваших пользователей необходимо фиксировать для того чтобы знать, нужно ли предпринимать дополнительные меры по обеспечению безопасности. Проверка такой информации с целью определения активности на предприятии называется аудитом.

Необходимо помнить, что по умолчанию параметр политики аудита для рабочих станций установлен на *«Не определено»***.** В общей сложности, вы можете настраивать девять политик аудита:

Настройка аудита входа в систему. Текущая политика определяет, будет ли операционная система пользователя, для компьютера которого применяется данная политика аудита, выполнять аудит каждой попытки входа пользователя в систему или выхода из нее. Например, при удачном входе пользователя на компьютер генерируется событие входа учетной записи. События выхода из системы создаются каждый раз, когда завершается сеанс вошедшей в систему учетной записи пользователя. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Настройка аудита доступа к объектам. Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к ActiveDirectory. К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом (SACL). Аудит создается только для объектов, для которых указаны списки управления доступом, при условии, что запрашиваемый тип доступа и

учетная запись, выполняющая запрос, соответствуют параметрам в данных списках.

Настройка аудита доступа к службе каталогов. При помощи этой политики безопасности вы можете определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне «Дополнительные параметры безопасности» свойств объекта ActiveDirectory. Аудит создается только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учетная запись, выполняющая запрос, соответствуют параметрам в данном списке. Данная политика в какой-то степени похожа на политику «Аудит доступа к объектам». Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту ActiveDirectory, для которого определена таблица SACL. Аудит отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту ActiveDirectory, для которого определена таблица SACL.

Настройка аудита изменения политики. Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователям, аудита, учетной записи или доверия. Аудит успехов означает создание записи аудита при каждом успешном изменении политик назначения прав пользователей, политик аудита или политик доверительных отношений. Аудит отказов означает создание записи аудита при каждой неудачной попытке изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Настройка аудита изменения привилегий. Используя эту политику безопасности, вы можете определить, будет ли выполняться аудит использования привилегий и прав пользователей. Аудит успехов означает создание записи аудита для каждого успешного применения права пользователя. Аудит отказов означает создание записи аудита для каждого неудачного применения права пользователя.

Настройка аудита отслеживания процессов. Текущая политика аудита определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам. Аудит успехов означает создание записи аудита для каждого успешного события, связанного с отслеживаемым процессом. Аудит отказов означает создание записи аудита для каждого неудачного события, связанного с отслеживаемым процессом.

Настройка аудита системных событий. Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики вы можете узнать, перегружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы

аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события.

Настройка аудита событий входа в систему. При помощи этой политики аудита вы можете указать, 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. Члены домена и компьютеры, не входящие в домен, являются доверенными для своих локальных учетных записей. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удаленного входа, причем события выхода из системы не записываются. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Настройка аудита управления учетными записями. Эта последняя политика тоже считается очень важной, так как именно при помощи нее вы можете определить, необходимо ли выполнять аудит каждого события управления учетными записями на компьютере. В журнал безопасности будут записываться такие действия как создание, перемещение и отключение учетных записей, а также изменение паролей и групп. Аудит успехов означает создание записи аудита для каждого успешного события управления учетными записями. Аудит отказов означает создание записи аудита для каждого неудачного события управления учетными записями.

Для настройки аудита вам нужно определить параметр политики. После двойного нажатия левой кнопкой мыши на любом из параметров, установите флажок на опции *«Определить следующие параметры политики»* и укажите параметры ведения аудита успеха, отказа или обоих типов событий. Для отказа от аудита необходимо снять на опции оба флажка.

4.6. ***Политика назначения прав пользователей***

a) Откройте оснастку *«Локальные политики безопасности»*;
b) Перейдите в узел «Локальные политики» и откройте параметр «Назначение прав пользователя».

Стоит учесть, что пользователи обычно не владеют достаточной базой знаний по обеспечению безопасности и даже у обычного пользователя может быть достаточно привилегий для нанесения ущерба своей системе и даже компьютерам в интрасети. Избежать подобных проблем помогают локальные политики безопасности назначения прав пользователя. При помощи политик назначения прав пользователя вы можете сами определить, для каких пользователей или групп пользователей будут предоставлены различные права и привилегии. Для назначения прав доступны 44 политики безопасности. Рассмотрим некоторые из политик:

Добавление рабочих станций к домену. Эта политика отвечает за разрешение пользователям или группам добавлять компьютеры в домен ActiveDirectory. Пользователь, обладающий данными привилегиями, может добавить в домен до десяти компьютеров. По умолчанию, все пользователи, прошедшие проверку подлинности, на контроллерах домена могут добавлять до десяти компьютеров.

Доступ к компьютеру из сети. Данная политика безопасности отвечает за разрешение подключения к компьютеру по сети указанным пользователям или группам. На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы»и«Операторы архивации»**,** «Пользователи»и «Все»**.**

Завершение работы системы. Используя этот параметр политики, вы можете составить список пользователей, которые имеют право на использование команды «Завершение работы» после удачного входа в систему. На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы»,«Операторы архивации»и«Пользователи» (только на рабочих станциях).

Запретить вход в систему через службу удаленных рабочих столов. При помощи данной политики безопасности вы можете ограничить пользователей или группы от входа в систему в качестве клиента удаленных рабочих столов. По умолчанию, как на рабочих станциях, так и на серверах, всем разрешено входить в систему как клиенту удаленных рабочих столов.

Запретить локальный вход. Данная политика запрещает отдельным пользователям или группам выполнять вход в систему. По умолчанию всем пользователям разрешен вход в систему.

Изменение системного времени. Эта политика отвечает за изменение системного времени. Предоставив данное право пользователям или группам, вы тем самым кроме разрешения изменения даты и времени внутренних часов позволите им изменять соответствующее время отслеживаемых событий в Журнале событий. На рабочих станциях и серверах данные привилегии предоставляются группам «Администраторы» и «Локальная служба».

4.7. *Журналы событий Windows*

В MicrosoftWindows*событие (event)* – это любое происшествие в операционной системе, которое записывается в журнал или требует уведомления пользователей или администраторов. Это может быть служба, которая не хочет запускаться, установка устройства или ошибка в работе приложения. События регистрируются и сохраняются в журналах событий Windows и предоставляют важные хронологические сведения, помогающие вести мониторинг системы, поддерживать ее безопасность, устранять ошибки и выполнять диагностику. Необходимо регулярно анализировать информацию, содержащуюся в этих журналах. Вам следует регулярно следить за журналами событий и настраивать операционную систему на сохранение важных системных событий. В том случае, если вы

администратор серверов Windows, то необходимо следить за безопасностью их систем, нормальной работой приложений и сервисов, а также проверять сервер на наличие ошибок, способных ухудшить производительность. Если вы пользователь персонального компьютера, то вам следует убедиться в том, что вам доступны соответствующие журналы, необходимые для поддержки своей системы и устранения ошибок. По умолчанию в операционной системе определен перечень событий, которые фиксируются в журналах. Дополнительно степень детализации событий определяется настройками политики аудита.

Приложение «Просмотр событий» можно открыть следующими способами:

a) Нажмите на кнопку «Пуск» для открытия меню, откройте «Панель управления», из списка компонентов панели управления выберите «Администрирование» и из списка административных компонентов стоит выбрать «Просмотр событий»;
b) Воспользоваться комбинацией клавиш WIN+R для открытия диалога «Выполнить» (или запустить диалог из меню кнопки «Пуск»). В диалоговом окне «Выполнить», в поле «Открыть» введите *eventvwr.msc* и нажмите на кнопку «ОК»;
c) Откройте «Консоль управления MMC». Для этого нажмите на кнопку «Пуск», в поле поиска введите *mmc*, а затем нажмите на кнопку «Enter». Откроется пустая консоль MMC. В меню «Консоль» выберите команду «Добавить или удалить оснастку»или воспользуйтесь комбинацией клавиш Ctrl+M. В диалоге **«Добавление и удаление оснасток»** выберите оснастку «Просмотр событий» и нажмите на кнопку «Добавить». Затем нажмите на кнопку «Готово», а после этого - кнопку «ОК»;

Стандартный набор включает 3 журнала:

Приложение – хранит важные события, связанные с конкретным приложением. Например, почтовый сервер сохраняет события, относящиеся к пересылке почты, в том числе события информационного хранилища, почтовых ящиков и запущенных служб.

Безопасность – хранит события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам.

Система – хранит события операционной системы или ее компонентов, например, неудачи при запусках служб или инициализации драйверов, общесистемные сообщения и прочие сообщения, относящиеся к системе в целом.

Желательно почаще просматривать журналы событий **«Приложение»** и **«Система»** и изучать существующие проблемы и предупреждения, которые могут предвещать о проблемах в будущем.

Для каждого журнала можно настроить его свойства. Для этого нужно выбрать журнал событий, а затем выбрать команду «Свойства» из меню «Действие» или из контекстного меню выбранного журнала.

В поле «Максимальный размер журнала (КБ)» установите требуемое значение при помощи счетчика или установите вручную без использования счетчика. В этом случае значение будет округлено до ближайшего числа, кратного 64 КБ, так как размер файла журнала должен быть кратен 64 КБ и не может быть меньше 1024 КБ.События сохраняются в файле журнала, размер которого может увеличиваться только до заданного максимального значения. После достижения файлом максимального размера, обработка поступающих событий будет определяться политикой хранения журналов:

- *Переписывать события при необходимости (сначала старые файлы)* – в этом случае новые записи продолжают заноситься в журнал после его заполнения. Каждое новое событие заменяет в журнале наиболее старое;
- *Не переписывать события (очистить журнал вручную)* – в этом случае журнал очищается вручную, а не автоматически.

В зависимости от версии операционной системы доступны другие политики хранения журнала.

5. Методические рекомендации по выполнению работ

5.1. *Управление встроенными учётными записями*

Для перехода к параметру «Управление встроенными учетными записями» выполним следующие действия: *сочетание клавиш «Win+R» -> ввод команды «secpol.msc» в появившемся окне «Выполнить» ->В открывшейся оснастке «Локальные политики безопасности» перейдем в узел «Локальные политики» -> Перейдем в узел «Параметры безопасности» (см. рис. 1).*

Мотивация: организации необходимо иногда предоставлять доступ людям, не являющимся сотрудниками, но имеющим необходимость воспользоваться вычислительными ресурсами. Для чего имеется специальная гостевая учетная запись «Гость». Название которой можно изменить в целях облегчения поиска гостевой учетной записи.

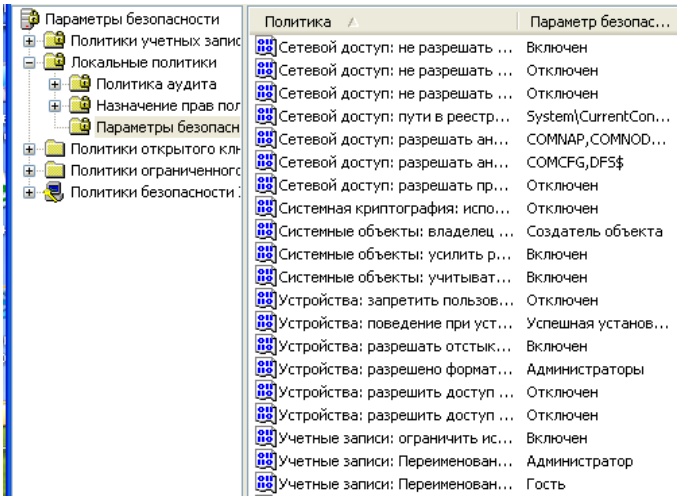


Рис.1.Параметры безопасности

Откроем параметр «Учетные записи: Переименование учетной записи». Встроенными учётными записями являются учётные записи гостя и администратора. В текстовом поле открывшегося окна введем имя гостевой записи «Гостевая запись» и нажмем кнопку «Ок» (рис.5.2).

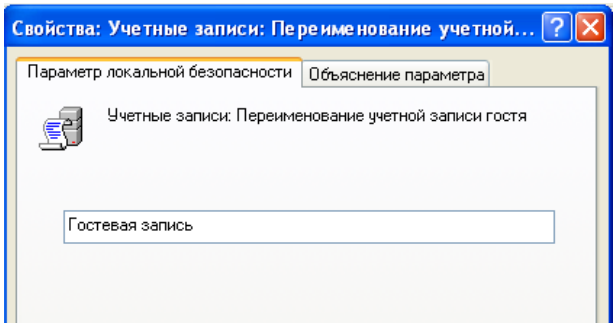


Рис.5.2.Создание гостевой записи

После этого перезапустим систему и проверим настройку. Если выполненные действия были осуществлены правильно, тогда, при открытии параметра «Учетные записи: Переименование учетной записи» можно наблюдать созданную ранее гостевую учетную запись (рис.5.3).

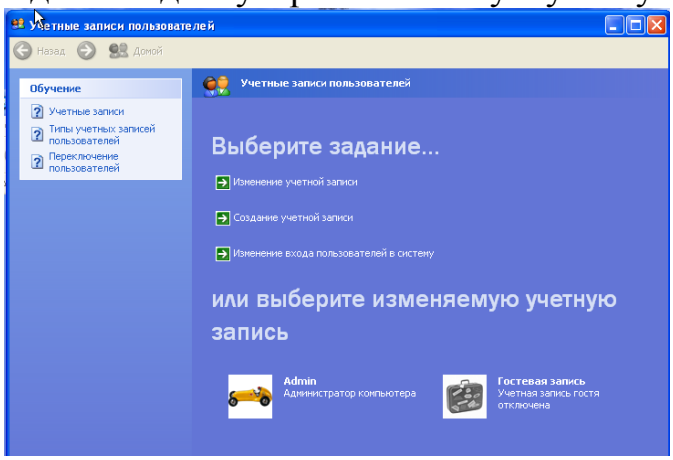


Рис.5.3. Окно "учетные записи пользователей"

Используя оснастку, можно переименовывать имя гостевого профиля системы и изменять состояние учетной записи между Вкл\Выкл. Данное действие может быть применено для изоляции доступа к системе от нежелательных пользователей.

По умолчанию запись «Гость» отключена, но если необходимо ее включить, то переименование этой учетной записи даст возможность повысить защищенность АРМ.

В качестве безопасности контура, созданная гостевая запись была отключена, чтобы злоумышленник не мог ею воспользоваться.

5.2. *Управление политиками паролей*

Чтобы настроить данные политики, необходимо:

сочетание клавиш «Win+R» -> ввод команды «secpol.msc» в появившемся окне «Выполнить» ->В открывшейся оснастке «Локальные политики

безопасности» перейдем в узел «Политики учетных записей» -> Перейдем в параметр «Политики паролей».

Мотивация: пользователи, имеющие цель компрометации учетных записей сотрудников, могут попытаться получить доступ к легитимным профилям через перебор паролей. Чтобы этого не произошло, необходимо ограничивать число попыток входа с некорректными учетными данными. Например, изменим срок действия пароля, минимальную длину пароля, зададим требования сложности, чтобы усложнить взлом устройства.

5.2.1. Максимальные срок действия пароля

Эта политика указывает период времени, в течение которого пользователь может использовать свой пароль до последующего изменения. По окончанию установленного срока пользователь обязан изменить свой пароль, так как без изменения пароля войти в систему ему не удастся. Доступные значения могут быть установлены в промежутке от 0 до 999 дней. Если установлено значения равное 0, срок действия пароля неограничен. Если значения максимального срока действия пароля варьируется от 1 до 999 дней, значение минимального срока должно быть меньше максимального. По умолчанию максимальный срок действия пароля 42 дня (рис.5.4).

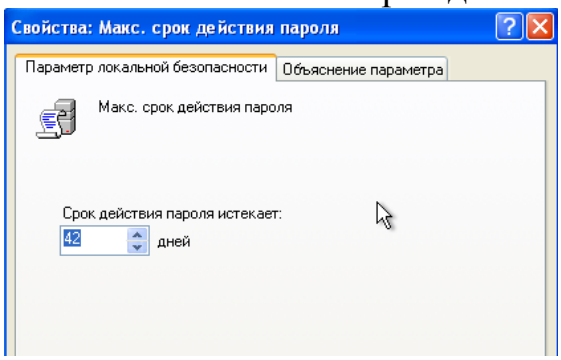


Рис.5.4. Максимальный срок действия пароля

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной. Однако, в целях безопасности хранящихся ресурсов, установим максимальный срок на 1 месяц (31 день) (рис. 5.5). Таким образом, нет необходимости в коротком максимальном сроке действия пароля. Короткий срок действия пароля приведёт к обязательной частой смене пароля. Однако устанавливать слишком длинный максимальный срок действия тоже не стоит, поскольку у злоумышленника будет больше времени для получения информации о пароле.

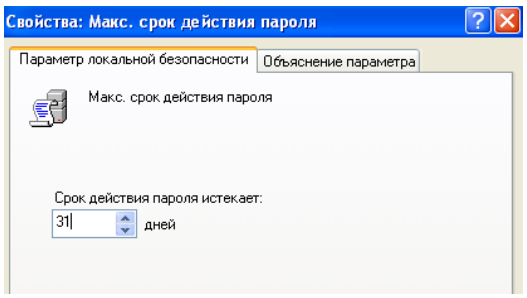


Рис.5.5 - Настройка максимального срока действия пароля

5.2.2. Минимальная длина пароля

При помощи этой политики можно указать минимальное количество знаков, которое должно содержаться в пароле. Если активировать этот параметр, то при вводе нового пароля количество знаков будет сравниваться с тем, которое установлено в этой политике. Если количество знаков будет меньше указанного, то придётся изменить пароль в соответствии с политикой безопасности. Можно указать значение политики от 1 до 14 знаков. По умолчанию минимальная длина пароля составляет 0 символов (рис. 5.6).

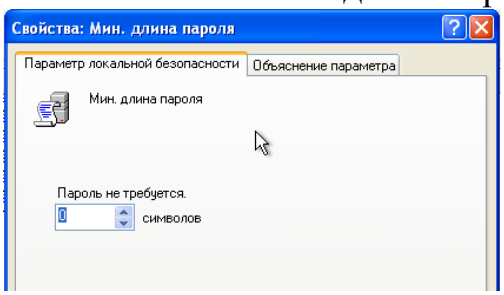


Рис.5.6. Минимальная длина пароля по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому необходимости в очень длинном пароле нет. Однако, в целях безопасности хранящихся ресурсов, использование совсем простых паролей недопустимо. Поэтому, установим значение данного параметра в 8 знаков (рис. 5.7).

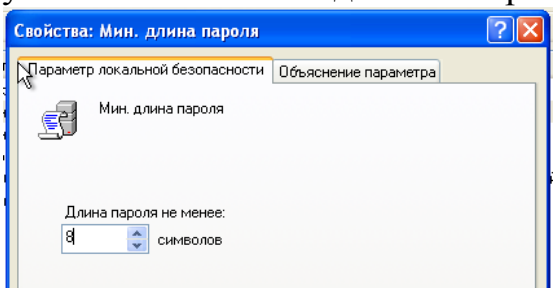


Рис.5.7.Настройка минимальной длины пароля

5.2.3. Минимальный срок действия пароля

Многие пользователи не захотят запоминать новый сложный пароль и могут попробовать сразу изменить его на свой старый хорошо известный первоначальный пароль. Для предотвращения подобных действий была разработана текущая политика безопасности. Можно указать минимальное количество дней, в течение которого пользователь должен использовать свой новый пароль. Доступные значения этой политики устанавливаются в промежутке от 0 до 998 дней. Установив значение равное 0 дней, пользователь сможет изменить пароль сразу после создания нового. Необходимо обратить внимание на то, что минимальный срок действия нового пароля не должен превышать значение максимального срока действия. По умолчанию, минимальный срок действия паролей установлен на 0 дней (рис. 5.8).

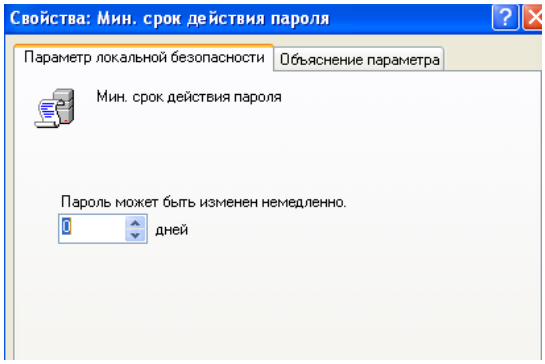
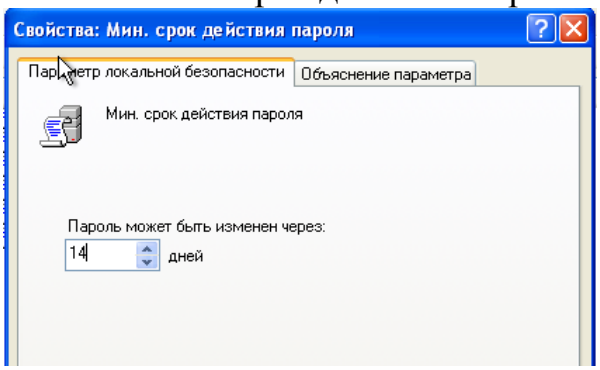


Рис.5.8. Минимальный срок действия пароля по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в большом минимальном сроке действия пароля. Частая смена пароля может привести к частым неудачным попыткам входа в систему, поскольку не все пользователи могут запомнить новый пароль. Однако, если задать большой минимальный срок действия пароля, это облегчит злоумышленнику задачу подбора пароля, поскольку, как правило, пользователи стараются использовать один и тот же пароль на нескольких учетных записей. Если злоумышленник сможет скомпрометировать пароль на иных ресурсах пользователя, он может попытаться использовать его для входа в защищаемую нами систему. Исходя из вышесказанного, установим минимальный срок действия пароля на 14 дней (рис. 5.9).



Рису.5. 9.Настройка минимального срока действия пароля

5.2.4. Пароль должен отвечать требованиям сложности

Это одна из самых важных политик паролей, которая отвечает за то, должен ли пароль соответствовать требованиям сложности при создании или изменении пароля. В связи с этими требованиями, пароли должны:

- содержать буквы верхнего и нижнего регистра одновременно;
- содержать цифры от 0 до 9;
- содержать символы, которые отличаются от букв и цифр (например,!, @, #, $, *);
- не содержать имени учётной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

По умолчанию данный параметр отключен (рис. 5.10).

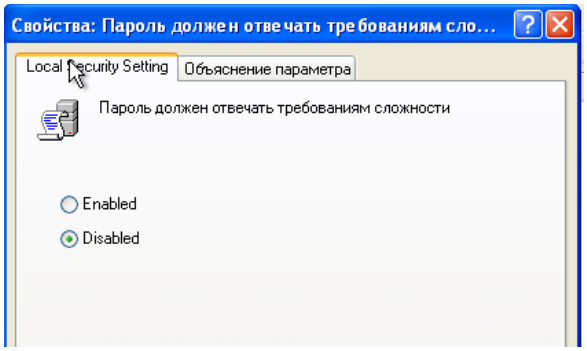


Рис.5.10.Параметр "Пароль должен отвечать требованиям сложности" по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в очень сложном пароле, однако перечисленные выше требования исключают возможность использования таких простых паролей, как, например, набор цифр или дата рождения. Использование таких паролей никак не осложнит злоумышленнику доступ к данным. Поэтому включим данный параметр на АРМ (рис. 5.1).

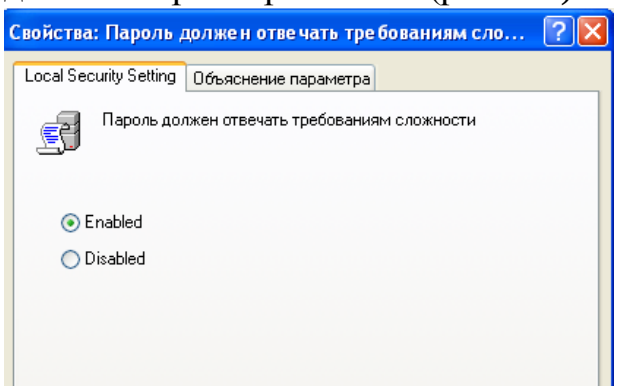


Рис.5.11. Настройка требований сложности пароля

5.2.5. Требованиенеповторяемости паролей

Указывается количество предыдущих паролей пользователя, с которыми будет сравниваться новый пароль. По умолчанию в параметр не настроен (0 хранимых паролей). (рис. 5.12).

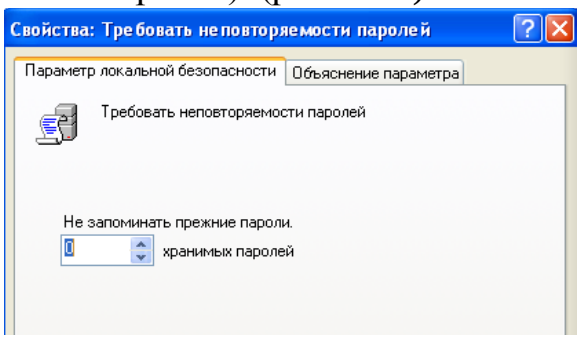


Рис.5.12.Настройка неповторяемости паролей по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в том, чтобы пользователи каждый раз придумывали новый пароль, однако, если пользователи будут постоянно использовать один и тот же пароль, то нет никакого смысла в настройке смены пароля, а также, как и в пункте ранее, подобная ситуация облегчит доступ злоумышленника к системе. Исходя из вышесказанного, настроем данный параметр на значение 5. Таким образом, пользователю необходимо будет придумать как минимум 6 новых паролей. (рис. 5.13).

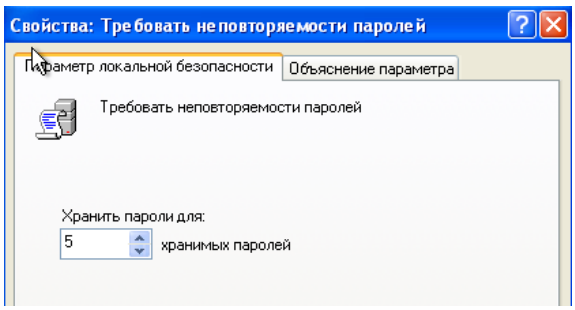


Рис.5.13.Настройка неповторяемости паролей

5.2.6. Хранение паролей, используя обратимое шифрование

Для того чтобы пароли невозможно было перехватить при помощи приложений, ActiveDirectory хранит только хэш-код. Но если возникнет необходимость поддержки приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности, можно использовать текущую политику. Обратимое шифрование по умолчанию отключено (рис. 5.14), так как, используя эту политику, уровень безопасности паролей и всего домена в частности значительно понижается. Использование этой функции аналогично хранению пароля в открытом виде.

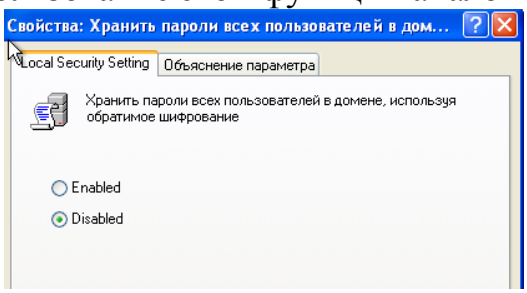


Рис.5.14. Параметр использования обратимого шифрования при хранении паролей по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому мы не будем включать обратимое шифрование, поскольку включение данной политики значительно понизит безопасность паролей.

5.3. ***Политики блокировки учётной записи***

Чтобы настроить данные политики, необходимо:

сочетание клавиш «Win+R» -> ввод команды «secpol.msc» в появившемся окне «Выполнить» -> В открывшейся оснастке «Локальные политики безопасности» перейдем в узел «Политики учетных записей» -> Перейдем в параметр «Политики блокировки учетных записей».

Мотивация: злоумышленник может быть не гостем, а легитимным сотрудником, имеющим неограниченные возможности при попытке входа в чужой профиль, тогда следует предпринять более решительные меры по ограничению опасной активности и заблокировать учетную запись, чтобы остановить потенциального нарушителя информационной безопасности. Например, после 10 попыток входа в систему.

Даже после создания сложного пароля и правильной настройки политик безопасности, учётные записи пользователей всё ещё могут быть подвергнуты атакам недоброжелателей.

Политики безопасности Windows могут противостоять этому, используя набор политик узла «Политика блокировки учётной записи». При помощи данного набора политик, появляется возможность ограничения количества некорректных попыток входа пользователя в систему. Разумеется, для пользователей это может быть проблемой, так как не у всех получится ввести пароль за указанное количество попыток, но зато безопасность учётных записей перейдет на «новый уровень». Для этого узла доступны только три политики.

5.3.1. Время до сброса счётчиков блокировки

ActiveDirectory и групповые политики позволяют автоматически разблокировать учётную запись, количество попыток входа в которую превышает установленное вами пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Можно установить значение от одной минуты до 99999. Это значение должно быть меньше значения политики «Продолжительность блокировки учётной записи». По умолчанию время блокировки учетной записи 30 минут. (рис. 5.15).

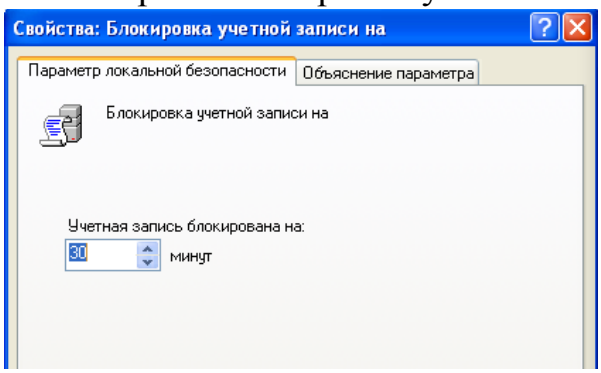


Рис.5.15.Время блокировки учетной записи по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в большом времени до сброса счётчиков блокировки, поэтому значение параметра в 60 минут будет вполне удовлетворительным (рис.5.16).

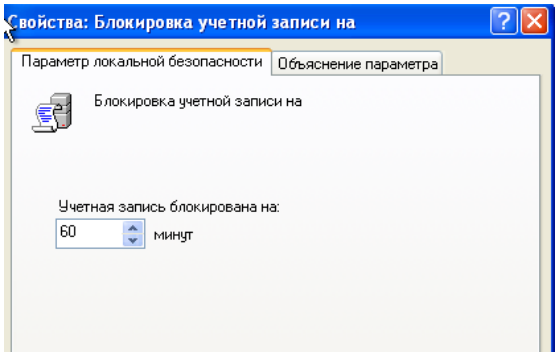


Рис.5.16. Настройка времени до сброса счётчиков блокировки

5.3.2. Пороговое значение блокировки

Используя эту политику, можно указать количество некорректных попыток входа, после чего учётная запись будет заблокирована. Окончание периода блокировки учётной записи задаётся политикой «Продолжительность блокировки учётной записи» или администратор может разблокировать учётную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. По умолчанию пороговое значение не установлено. (рис. 5.17).

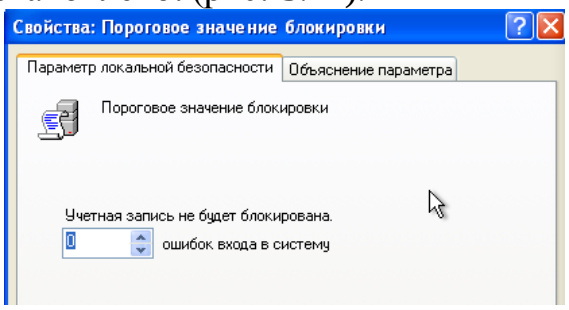


Рис.5.17 - Пороговое значение по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в малом пороговом значении блокировки. Зададим пороговое значение «5», таким образом, если пользователи введут 5 раз неверный пароль, учетная запись будет заблокирована. (рис. 5.18).

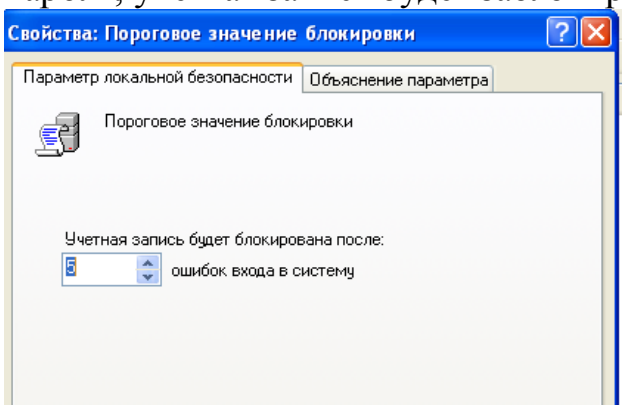


Рисунок 18 - Настройка порогового значения блокировки

5.3.3. Продолжительность блокировки учётной записи

При помощи этого параметра вы можете указать время, в течение которого учётная запись будет заблокирована до её автоматической разблокировки. Можно установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0, учётная запись будет заблокирована до тех пор, пока администратор не разблокирует её вручную. По умолчанию продолжительность блокировки учетной записи равна 30 минутам. (рис. 5.19)

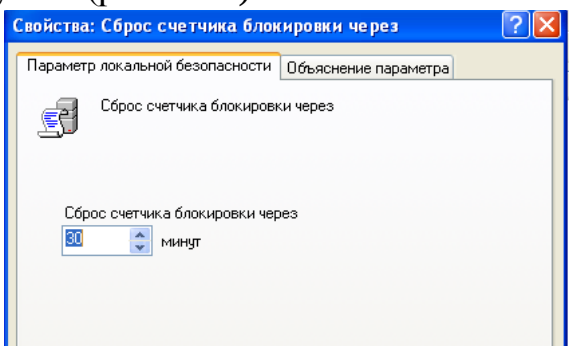


Рис.5.19 - Продолжительность блокировки по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в долгом времени блокировки учётной записи пользователя, поэтому значение параметра в 60 минут будет вполне удовлетворительным (рис. 5.20).

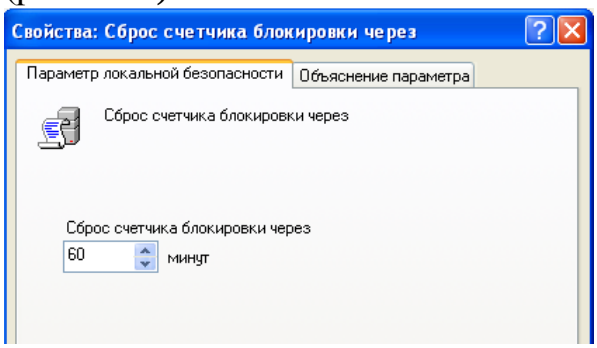


Рис.5.20 - Настройка продолжительности блокировки учётной записи

5.4. ***Политика аудита***

Чтобы настроить данные политики, необходимо:
сочетание клавиш «Win+R» -> ввод команды «secpol.msc» в появившемся окне «Выполнить» -> В открывшейся оснастке «Локальные политики безопасности» перейдем в узел «Локальные политики» -> Перейдем в параметр «Политика аудита».

После того как политики безопасности учётных записей у вас правильно настроены, злоумышленникам будет намного сложнее получить доступ к пользовательским учётным записям. Но не стоит забывать о том, что на этом работа по обеспечению безопасности сетевой инфраструктуры не заканчивается. Все попытки вторжения и неудачную аутентификацию пользователей необходимо фиксировать для того чтобы знать, нужно ли предпринимать дополнительные меры по обеспечению безопасности.

Проверка такой информации с целью определения активности на предприятии называется аудитом.

Мотивация: нарушитель все еще может являться сотрудником организации, имеющим цель нанести ущерб организации через использование своих привилегий, тогда для обеспечения информационной безопасности может пригодиться аудит действий сотрудников, при правильной настройке политики которого будет производиться запись подозрительных действий в журнал. Например, уделять особое внимание, когда пользователь пытается запустить файлы, требующие административного доступа. Правильная организация политики аудита может облегчить выявление злоумышленников, находящихся среди доверенных пользователей системы. Для этого необходимо определиться, какие события подходят для аудита нежелательной активности пользователя.

Необходимо помнить, что по умолчанию параметр политики аудита для рабочих станций установлен на «Не определено».

5.4.1. Аудит входа в систему

Текущая политика определяет, будет ли операционная система пользователя, для компьютера которого применяется данная политика аудита, выполнять аудит каждой попытки входа пользователя в систему или выхода из неё. Например, при удачном входе пользователя на компьютер генерируется событие входа учётной записи. События выхода из системы создаются каждый раз, когда завершается сеанс вошедшей в систему учётной записи пользователя. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему. По умолчанию аудита нет. (рис. 5.21).

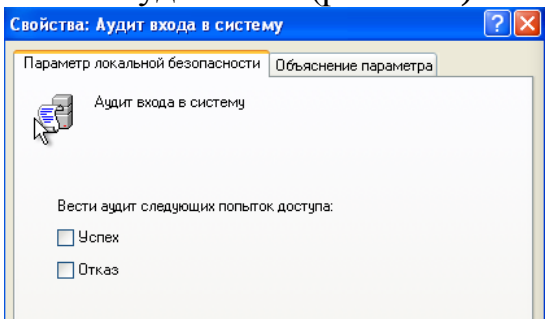


Рис.5.21.Аудит входа в систему по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в аудите успехов. Аудит отказов в данном случае будет полезным: используя эту настройку можно найти проблему, а также обнаружить нарушителя. (рис. 5.22).

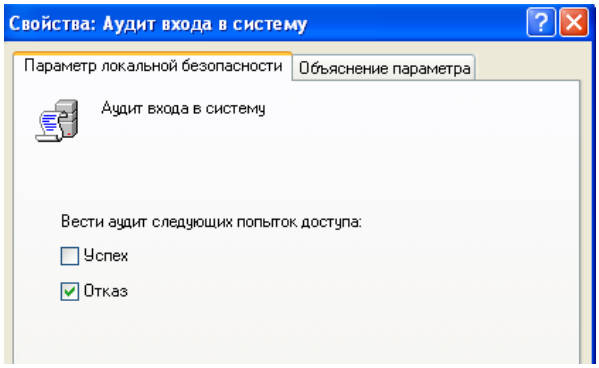


Рис.5.22. Настройка аудита входа в систему

5.4.2. Аудит доступа к объектам

Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к ActiveDirectory. К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом (SACL). Аудит создаётся только для объектов, для которых указаны списки управления доступом, при условии, что запрашиваемый тип доступа и учётная запись, выполняющая запрос, соответствуют параметрам в данных списках. По умолчанию аудита нет. (рис. 5.23).

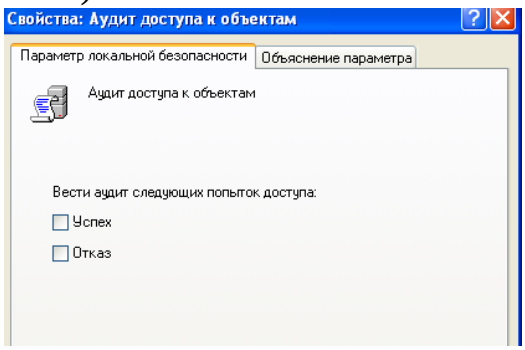


Рис.5.23.Аудит доступа к объектам по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в аудите успехов доступа к объектам, тем более что учётная запись, выполняющая запрос, соответствует параметрам в SACL. Однако аудит отказов будет полезным: он поможет как найти проблему, так и обнаружить нарушителя. Поэтому включим только аудит отказов (рис. 5.24).

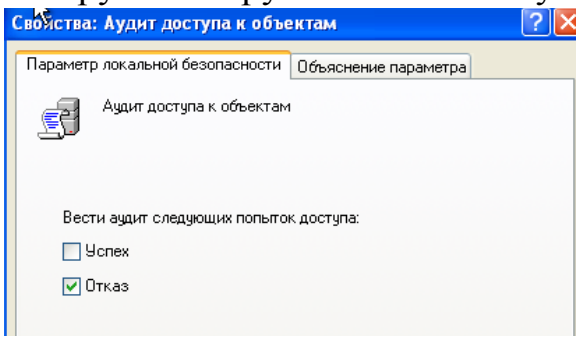


Рис.5.24 - Настройка аудита доступа к объектам

5.4.3. *Аудит доступа к службе каталогов*

При помощи этой политики безопасности вы можете определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне «Дополнительные параметры безопасности» свойств объекта ActiveDirectory. Аудит создается только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учётная запись, выполняющая запрос, соответствуют параметрам в данном списке. Данная политика в какой-то степени похожа на политику «Аудит доступа к объектам». Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту ActiveDirectory, для которого определена таблица SACL. Аудит отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту ActiveDirectory, для которого определена таблица SACL. По умолчанию аудита нет (рис. 5.25).

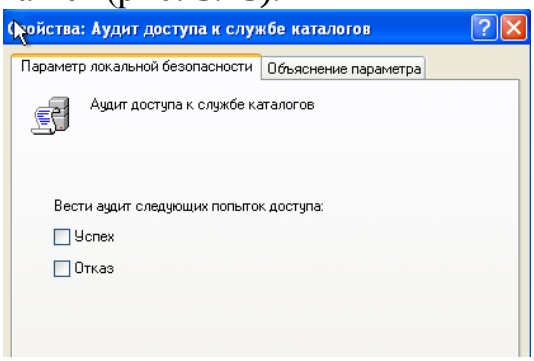


Рис.5.25 - Аудит доступа к каталогам по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в аудите успехов доступа к объектам, тем более что учётная запись, выполняющая запрос, соответствует параметрам в SACL. Однако аудит отказов будет полезным: он поможет как найти проблему, так и обнаружить нарушителя. Поэтому включим только аудит отказов (рис. 5.26).

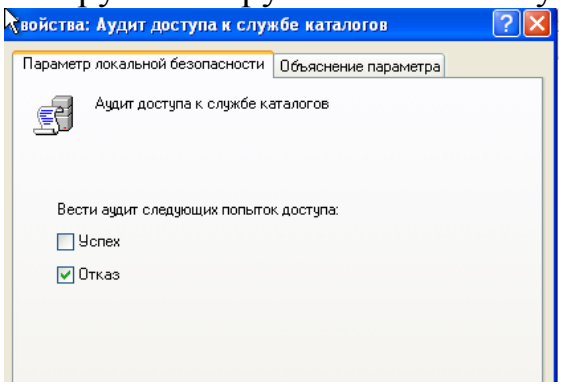


Рис.5.26.Настройка аудита доступа к службе каталогов

5.4.4. *Аудит изменения политики*

Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав

пользователям, аудита, учётной записи или доверия. Аудит успехов означает создание записи аудита при каждом успешном изменении политик назначения прав пользователей, политик аудита или политик доверительных отношений. Аудит отказов означает создание записи аудита при каждой неудачной попытке изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений. По умолчанию аудита нет. (рис.5. 27)

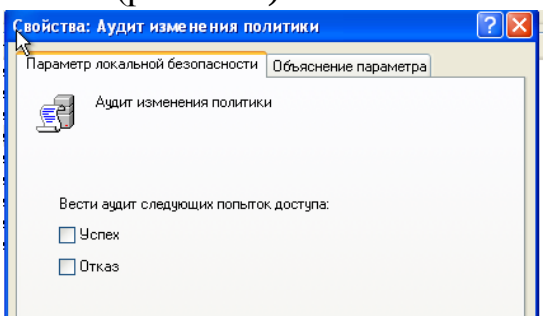


Рис.5.27.Аудит изменения политики по умолчанию

Несмотря на то, в настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, включим полный аудит, то есть и аудит отказов, и аудит успехов, поскольку потенциальные последствия несанкционированного изменения политик влекут за собой возможности злоумышленника к изменения личной информации, а также к повышению прав пользователя. (рис. 5.28).

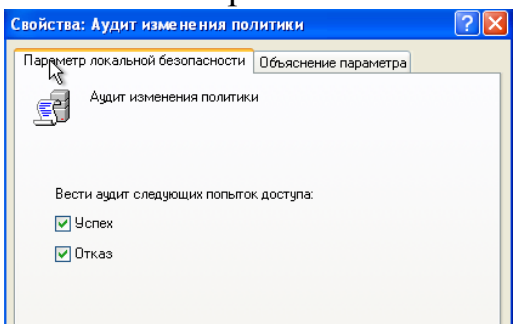


Рис.5.28.Настройка аудита изменения политик

5.4.5. *Аудит изменения привилегий*

Используя эту политику безопасности, можно определить, будет ли выполняться аудит использования привилегий и прав пользователей. Аудит успехов означает создание записи аудита для каждого успешного применения права пользователя. Аудит отказов означает создание записи аудита для каждого неудачного применения права пользователя. По умолчанию аудита нет. (рис. 5.29).

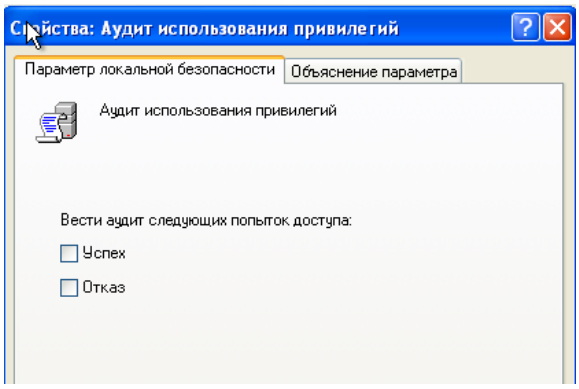


Рис.5.29. Аудит использования привилегий по умолчанию

Несмотря на то, в настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, включим полный аудит, то есть и аудит отказов, и аудит успехов. Причиной этому послужили потенциальные последствия несанкционированного изменения привилегий, например, приложение, обладающее большими полномочиями, чем предполагалось системным администратором, может совершать неавторизированные действия. (рис. 5.30).

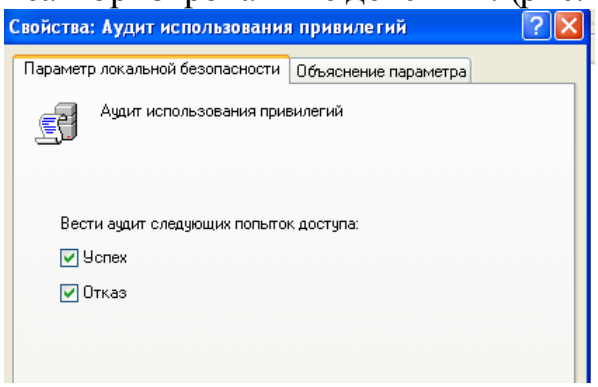


Рис.5.30. Настройка аудита изменения привилегий

5.4.6. Аудит отслеживания процессов

Текущая политика аудита определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам. Аудит успехов означает создание записи аудита для каждого успешного события, связанного с отслеживаемым процессом. Аудит отказов означает создание записи аудита для каждого неудачного события, связанного с отслеживаемым процессом. По умолчанию аудита нет. (рис. 5.31).

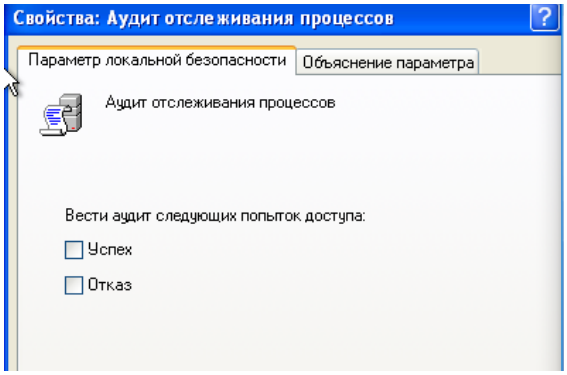


Рис.5.31.Аудит отслеживания процессов по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в аудите успехов. Аудит отказов в данном случае будет полезным: используя эту настройку можно найти проблему, а также обнаружить нарушителя. (рис. 5.32).

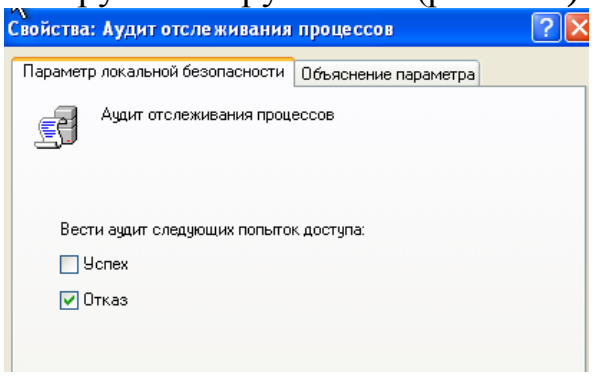


Рис.5.32. Настройка аудита отслеживания процессов

5.4.7. Аудит системных событий

Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики возможно узнать, перезагружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события. По умолчанию аудита нет. (рис. 5.33).

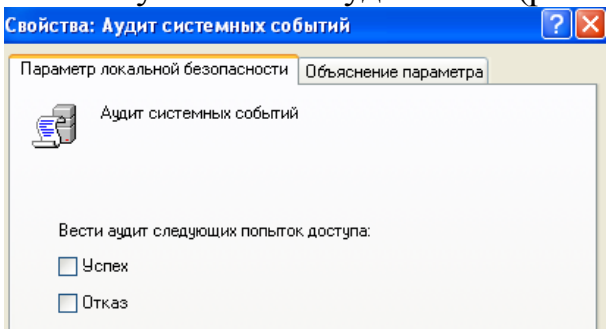


Рис.5.33. Аудит системных событий по умолчанию

Несмотря на то, в настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, включим полный аудит, то есть и аудит отказов, и аудит успехов. Причиной этому послужила большая роль этой политики в поиске проблем и причин неполадок. (рис. 5.34)

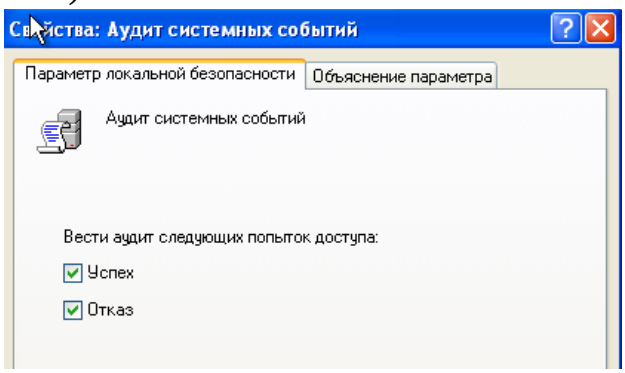


Рис.5.34. Настройка аудита системных событий

5.4.8. Аудит событий входа в систему

При помощи этой политики аудита возможно указать, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учётных данных. При использовании этой политики создается событие для локального и удалённого входа пользователя в систему. Члены домена и компьютеры, не входящие в домен, являются доверенными для своих локальных учётных записей. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удалённого входа, причём события выхода из системы не записываются. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему. По умолчанию аудита нет(рис. 5.35)

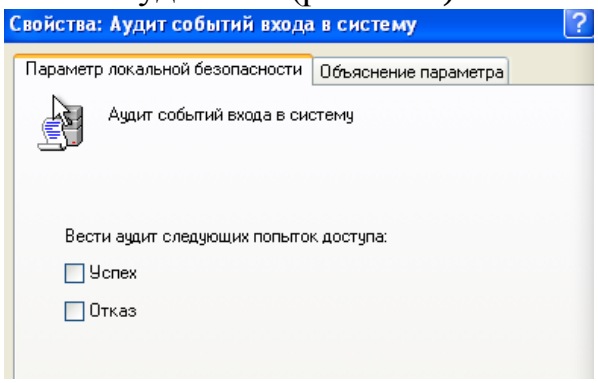


Рис.5.35. Аудит событий входа в систему по умолчанию

В настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, поэтому нет необходимости в аудите успехов. Аудит отказов в данном случае будет полезным: используя эту настройку можно найти проблему, а также обнаружить нарушителя (рис. 5. 36)

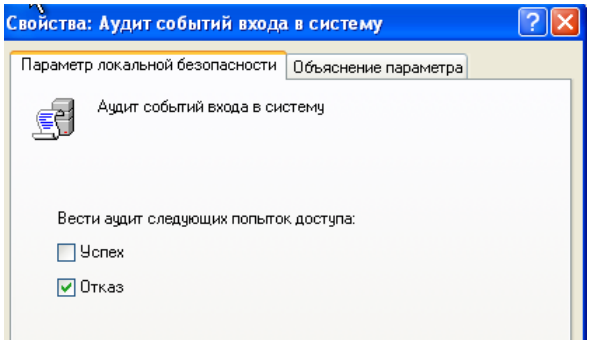


Рис.5.36. Настройка аудита событий входа в систему

5.4.9. Аудит управления учётными записями

Эта последняя политика также считается очень важной, так как именно при помощи нее можно определить, необходимо ли выполнять аудит каждого события управления учётными записями на компьютере. В журнал безопасности будут записываться такие действия как создание, перемещение и отключение учётных записей, а также изменение паролей и групп. Аудит успехов означает создание записи аудита для каждого успешного события управления учётными записями. Аудит отказов означает создание записи аудита для каждого неудачного события управления учётными записями. По умолчанию аудита нет (рис. 5.37).

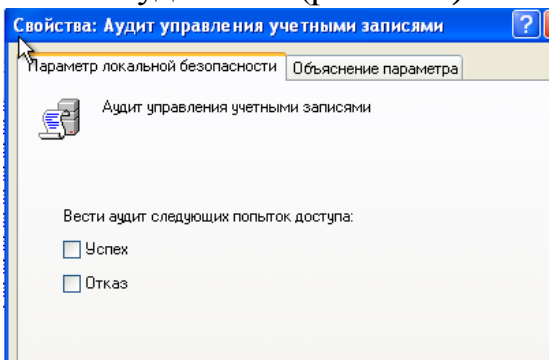


Рис. 5.37. Аудит управления учетными записями по умолчанию

Несмотря на то, в настраиваемом АРМ хранящаяся информация, к которой осуществляется доступ, является общедоступной, включим полный аудит, то есть и аудит отказов, и аудит успехов. Причиной этому послужила большая роль этой политики в поиске проблем и причин неполадок. (рис. 5.38).

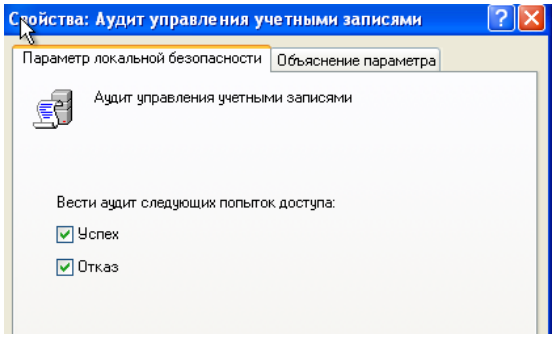


Рис. 5.38. Настройка аудита управления учётными записями

5.5. ***Политика назначения прав пользователей***

Чтобы настроить данные политики, необходимо:
сочетание клавиш «Win+R» -> ввод команды «secpol.msc» в появившемся окне «Выполнить» -> В открывшейся оснастке «Локальные политики безопасности» перейдем в узел «Локальные политики» -> Перейдем в параметр «Назначение прав пользователя».
Мотивация: каждому пользователю должны быть назначены администратором ИС конкретные права в соответствии с его ролью в бизнес-процессе.

Однако, даже у обычного пользователя может быть достаточно привилегий для нанесения ущерба ИС, включая удаленные ресурсы корпоративной сети. Избежать подобных проблем помогают настройки параметров локальных политик безопасности «Назначения прав пользователя». При помощи указанных политик можно определятьдля какихпользователей и/или групп пользователей предоставлены права и привилегиив ИС для выполнения делегированных им ролей в бизнес-процессе, что существенно повышает безопасность системы в целом. Для назначения прав доступны 44 политики безопасности. Рассмотрим 3 наиболее актуальных из них.

5.5.1. *Изменение системного времени*

Это право пользователя определяет, какие пользователи и группы могут изменять время и дату на встроенных часах компьютера. Пользователи, обладающие данным правом, могут изменять представление журналов безопасности. При изменении системного времени события будут заноситься в журнал с указанием заданного, а не реального времени. Данное право пользователя определено в объекте групповой политики стандартного контролера домена, а также в локальной политике безопасности рабочих станций и серверов. По умолчанию: "Администраторы", "Опытные пользователи"(рис. 5.39)

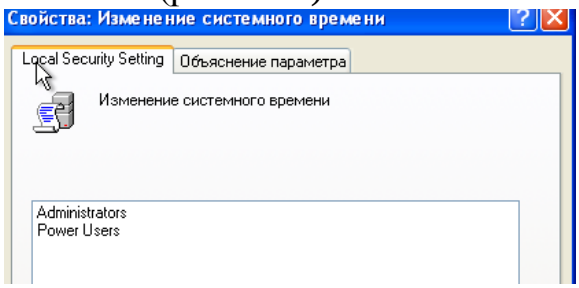


Рис. 5.39. Изменение системного времени по умолчанию

Так как изменение системного времени является операцией, которая может серьезно повлиять на работоспособность системы, то удалим все ненужные группы пользователей из списка тех групп, которые могут выполнять данное действие. То есть удалим группу «PowerUsers», потому что нарушитель может создать учётную запись, добавить её в эту группу, которая имеет название по умолчанию, поле чего у нарушителя появится возможность изменять системное время, что может привести к неполадкам и нарушению работы системы (рис. 5.40).

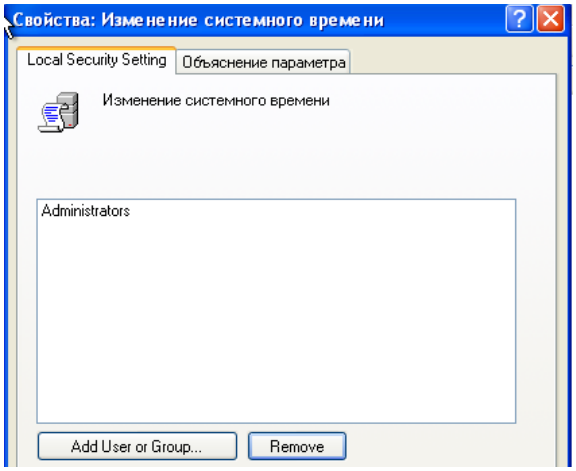


Рис. 5.40.Настройка права изменения системного времени

5.5.2. Завершение работы системы

Этот параметр безопасности определяет, какие пользователи могут, войдя на локальный компьютер, завершить работу операционной системы с помощью команды "Завершение работы". Неправильное использование этого права может привести к атаке типа "отказ в обслуживании". По умолчанию следующие группы могут завершать работу операционной системы: «*Administrators*», «*BackupOperators*», «*PowerUsers*», «*Users*». (рис. 5.41)

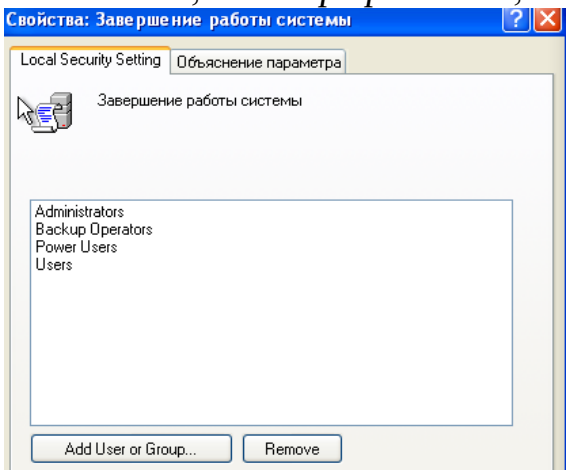


Рис. 5.41. Завершение работы системы по умолчанию

Так как завершение работы системы является операцией, которая может серьезно повлиять на работоспособность системы, то удалим все группы пользователей, кроме группы «*Administrators*» из списка тех групп, которые могут выполнять данное действие (рис. 5.42).

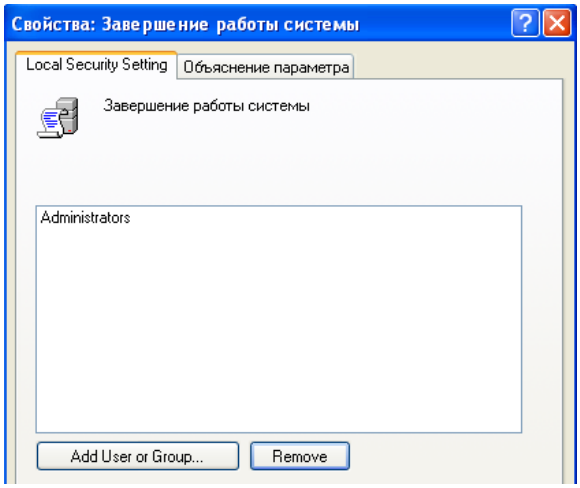


Рис. 5.42. Настройка права завершения работы системы

5.5.3. Разрешать вход в систему через службу терминалов

Этот параметр безопасности определяет, каким пользователям и группам разрешается входить в систему в качестве клиента служб терминалов. По умолчанию разрешается вход в систему в качестве клиента службы терминалов 2 группам пользователей: «*Administrators*» и «*RemoteDesktopUsers*». (рис. 5.43)

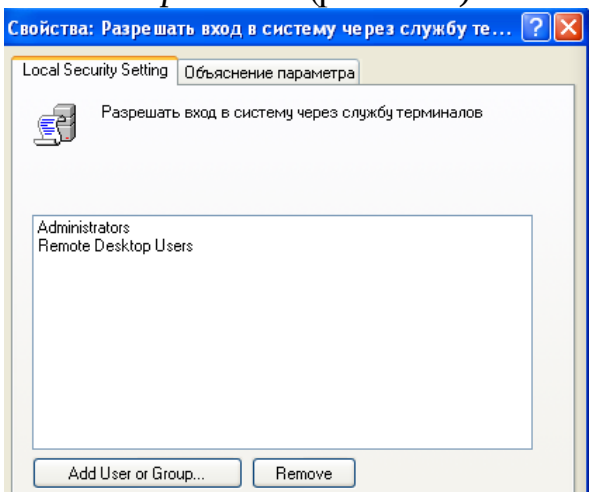


Рис. 5.43. Разрешение входа в систему через службу терминалов по умолчанию

Так как вход в систему через службу терминалов является операцией, которая может серьезно повлиять на работоспособность системы, то удалим группу «*RemoteDesktopUsers*» из списка тех групп, которые могут выполнять данное действие (рис. 5.44).

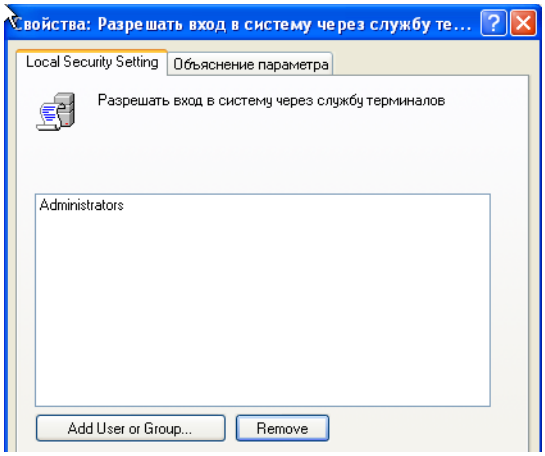


Рис.5.44. Настройка права завершения работы системы

5.6. *Журналы событий Windows*

В MicrosoftWindows событие (*event*) – это любое происшествие в операционной системе, которое записывается в журнал или требует уведомления пользователей или администраторов. События регистрируются и сохраняются в журналах событий Windows и предоставляют важные хронологические сведения, помогающие вести мониторинг системы, поддерживать её безопасность, устранять ошибки и выполнять диагностику.
Мотивация: при расследовании инцидентов информационной безопасности необходима возможность проведения тщательного анализа с сопоставлением во времени всех действий предполагаемого нарушителя. Увеличение размера журнала событий Windows способствует выявлению диструктивной активности на большем временном отрезке.

По умолчанию в ОС Windowsопределён перечень событий, которые фиксируются в журналах. Дополнительно степень детализации событий определяется настройками политики аудита.

Чтобы открыть приложение «Просмотр событий», требуется:
сочетание клавиш «Win+R» -> ввод команды «eventvwr.msc» в появившемся окне «Выполнить» -> нажать кнопку «Ok».

Стандартный набор включает 3 журнала:

- **Приложение** – хранит важные события, связанные с конкретным приложением. Например, почтовый сервер сохраняет события, относящиеся к пересылке почты, в том числе события информационного хранилища, почтовых ящиков и запущенных служб.
- **Безопасность** – хранит события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам.
- **Система** – хранит события операционной системы или ее компонентов, например, неудачи при запусках служб или инициализации драйверов,

общесистемные сообщения и прочие сообщения, относящиеся к системе в целом.

Желательно почаще просматривать журналы событий «Приложение» и «Система» и изучать существующие проблемы и предупреждения, которые могут предвещать о проблемах в будущем.

Для каждого журнала можно настроить его свойства. Для этого нужно выбрать журнал событий, а затем выбрать команду «Свойства» из меню «Действие» или из контекстного меню выбранного журнала.

В поле «Максимальный размер журнала (КБ)» установить требуемое значение при помощи счётчика или установить вручную без использования счётчика. В этом случае значение будет округлено до ближайшего числа, кратного 64 КБ, так как размер файла журнала должен быть кратен 64 КБ и не может быть меньше 1024 КБ. По умолчанию максимальный размер журнала 512 КБ (рис. 5.45).

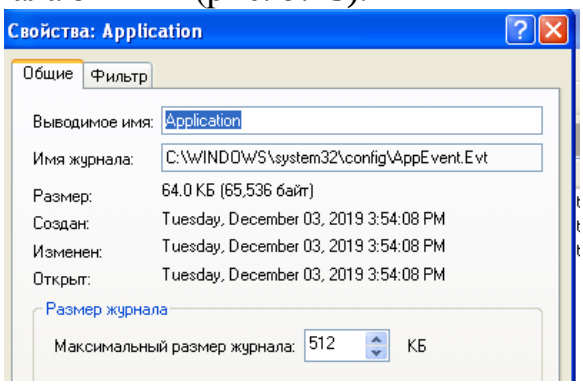


Рис.5.45. Настройка максимального размера журнала

Зададим максимальный размер журнала 1024 КБ (рис. 5.46).

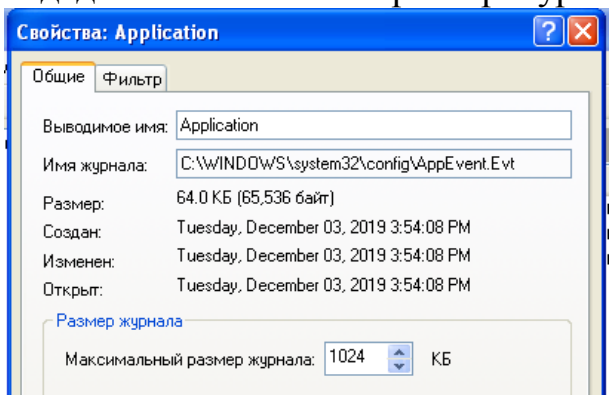


Рис.5.46. Максимальный размер журнала

События сохраняются в файле журнала, размер которого может увеличиваться только до заданного максимального значения. После достижения файлом максимального размера, обработка поступающих событий будет определяться политикой хранения журналов:

Переписывать события при необходимости (сначала старые файлы) – в этом случае новые записи продолжают заноситься в журнал после его заполнения. Каждое новое событие заменяет в журнале наиболее старое;

Не переписывать события (очистить журнал вручную) – в этом случае журнал очищается вручную, а не автоматически.

По умолчанию переписываются события старее 7 дней (рис. 5.47)

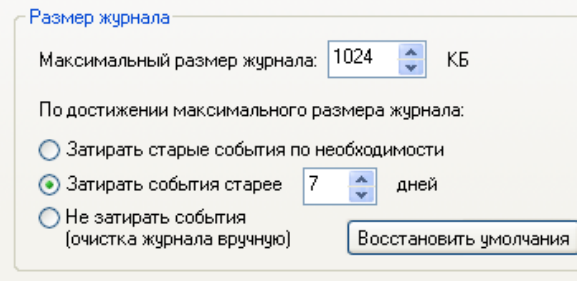


Рис. 5.47. Настройка действий по достижении максимального размера журнала по умолчанию

Так как в настраиваемый АРМ записей в журнале событий будет много, потому что АРМ обыкновенно может иметь как множество пользователей, так и множество приложений, - выберем вариант (старее 5 дней) переписывать события при необходимости (рис. 5.48).

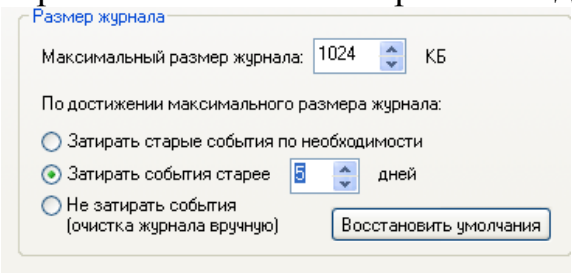


Рис.5.48. Настройка действий по достижении максимального размера журнала

Выводы. В результате лабораторной работы была произведена настройка локальных политик безопасности АРМ с установленной ОС WindowsXP и расположенного в «открытом» контуре.

Обоснование выбора и настройки параметров локальных политик безопасности базируются на требованиях к защите АРМ от НСД в «открытом» контуре.

6. Содержание отчета

1. Цель выполнения работы
2. Теоретические положения
3. Процесс выполнения работы
4. Полученные результаты

4.1. Пояснения критериев выбора политик безопасности (4.2-4.7) для защиты АРМ от НСД в «закрытом» и «открытом» контуре.

4.2. Обоснование настроек каждого параметра соответствующих локальных политик безопасности в «закрытом» и «открытом» контуре.

4.3. Скриншоты до и после настройки параметров соответствующих политик безопасности.

5. Вывод о значимости настроек локальных политик безопасности для защиты АРМ от НСД.

7. Контрольные вопросы

7.1. На каких механизмах должно базироваться управление доступом в АРМ?

7.2. Какие требования защиты от НСД должны обеспечивать СЗИ от НСД в минимальной конфигурации, устанавливаемые на АРМ пользователей?
7.3. Какие запреты на действия пользователя АРМ должны налагать настройки СЗИ от НСД?
7.4. Что представляют собой локальные политики безопасности АРМ?
7.5. Какая оснастка используется для настройки локальной политики безопасности на автономном АРМ?
7.6. Объяснить критерии выбора политик безопасности (4.2-4.7) для защиты АРМ от НСД в «закрытом» и «открытом» контуре.
7.7. Обосновать настройки каждого параметра в локальных политиках безопасности (4.2-4.7) в «закрытом» и «открытом» контуре:
   a. *Управление встроенными учетными записями*
   b. *Управление политикой паролей*
   c. *Управление политикой блокировки учетной записи*
   d. *Управление политикой аудита*
   e. *Управление политикой назначения прав пользователей*
   f. *Управление политикой журналов событий Windows*

ЛАБОРАТОРНАЯ РАБОТА № 2
НАСТРОЙКА ГРУППОВЫЕЫХ ПОЛИТИК БЕЗОПАСНОСТИ АРМ

1. Цель работы

Цель работы – изучить редактор локальной групповой политики и научиться настраивать групповые политики безопасности на АРМ пользователя с установленной на нем ОС Windows для защиты информации от несанкционированного доступа (НСД).

Используемое программное обеспечение: ОС версии не ниже Windows XP.

2. Задание к выполнению работы

2.1. Установить макет варианта лабораторной работы на диск С (VirtualBox).
2.2. Провести настройки опций и политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя». При настройке опции «Сценарий» использовать сценарии на языках программирования и сценарии PowerShell (в пункте контекстного меню для свойства «Автозагрузка» выбрать вкладку – «Сценарии PowerShell».
2.3. Пояснить критерии выбора политик безопасности.
2.4. Обосновать настройки каждого параметра групповых политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя».
2.5. При настройке параметров соответствующих групповых политик безопасности указать последовательность команд для выхода в диалоговые

окна настройки параметров для каждой политики безопасности дочерних узлов. Пример: Откроем «Редактор локальной групповой политики», перейдя по адресу: «Конфигурация компьютера»→«Конфигурация Windows»→«Параметры безопасности» → «Политики учетных записей» →«Политики паролей».

2.6. Привести скриншоты до и после настройки параметров групповых политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя». Для опции «Сценарий» привести скриншоты сценариев на языках программирования и сценариев PowerShell (в пункте контекстного меню для свойства «Автозагрузка» выбрать вкладку – «Сценарии PowerShell».

3. Краткие теоретические сведения

3.1. *Введение в групповые политики Windows*

Групповые политики – это совокупность параметров, используемых для конфигурирования рабочего окружения пользователя или компьютера. Механизм групповых политик – основа централизованного управления конфигурациями пользователей (для разделения ресурсов между несколькими пользователями, использующих один компьютер) и компьютеров в корпоративной сети. В домашних условиях вы можете просто применить к своему компьютеру и необходимым учетным записям реестра, при помощи которых большинство настроек будут применены после перезагрузки компьютера или настраивать его вручную, что может занять очень много времени. Но как же быть, если вы работаете администратором в крупной организации, где нужно настроить десятки, а может и сотни компьютеров? Причем, в вашей организации, скорее всего, существует несколько отделов, у каждого из которых должны быть индивидуальные настройки. Например, компьютеры, расположенные в конференц-залах, предназначенные для проведения презентаций должны быть оснащены обоями рабочего стола с корпоративным логотипом. Или сотрудники отдела маркетинга не должны иметь права на запуск оснастки служб системы или редактора системного реестра. Большинство настроек локального компьютера или автоматизированного рабочего места (АРМ) пользователя, а также сетевых АРМ, которые входят в состав доменной сети, настраиваются при помощи групповых политик.

Групповые политики - это набор правил, обеспечивающих инфраструктуру, в которой администраторы локальных компьютеров и доменных служб ActiveDirectory могут централизовано развертывать и управлять настройками пользователей и компьютеров в организации. Все настройки учетных записей, операционной системы, аудита, системного реестра, параметров безопасности, установки программного обеспечения и прочие параметры развертываются и обновляются в рамках домена при помощи параметров объектов групповой политики GPO (GroupPolicyObject).

Объект групповой политики (англ. GroupPolicyObject, GPO) состоит из двух физически раздельных составляющих: контейнера групповой политики (англ. Group Policy Container, GPC) ишаблонагрупповойполитики (англ. Group Policy Template, GPT). Эти два компонента содержат в себе все данные о параметрах рабочей среды, которая включается в состав объекта групповой политики. Продуманное применение объектов GPO к объектам каталога ActiveDirectory позволяет создавать эффективную и легко управляемую компьютерную рабочую среду на базе ОС Windows. Политики применяются сверху вниз по иерархии каталога ActiveDirectory.

Групповые политики являются компонентом операционной системы Windows и основываются на тысячах отдельных параметров политик, иначе говоря, политик, определяющих определённую конфигурацию для своего применения.

3.2. *История групповых политик*

Структура многопользовательских операционных систем предполагает возможность создания для отдельного пользователя индивидуального окружения. В окружение пользователя могут входить: конфигурации рабочего стола и индивидуальные настройки оболочки; доступные пользователю приложения; сценарии, выполняющиеся при входе пользователя в системе или выходе из нее; ассоциированные с пользователем права и разрешения на доступ к локальным и сетевым информационным ресурсам. Для управления правами пользователей в доменах Windows и применяются механизмы групповых политик.

Для операционных систем Windows концепция групповых политик не является инновационным шагом в области системной безопасности и настройки операционных систем. Первые политики появились еще в Windows NT 4.0 и назывались системными политиками. Эти политики предназначались только для изменения данных системного реестра и основывались на файлах, которые назывались шаблонами adm. Для создания этих политик использовался специальный редактор системных политик. На то время системные политики были значительным шагом в обеспечении безопасности операционных систем Windows, несмотря на то, что объекты локальной политики не использовались, и система Windows NT 4.0 не поддерживала службы ActiveDirectory.

Групповые политики появились в операционной системе Windows 2000 и включали в себя около 900 настроек для пользователей и компьютеров, которые могли в полной мере применяться к клиентским компьютерам. Из утилиты, предназначенной для изменения данных системного реестра, групповые политики операционной системы Windows 2000 превратились в компонент, предназначенный для изменения параметров конфигурации операционной системы. Групповые политики по-прежнему расположены в шаблонах ADM. Система Windows 2000 Server уже позволяет распространять

объекты групповых политик для компьютеров, расположенных в домене и подразделениях (OU) в ActiveDirectory.

В операционных системах Windows XP и WindowsServer 2003 возможности групповых политик были расширены. С появлением этих систем у администраторов появилась возможность управлять параметрами безопасности и установкой приложений, а количество политик увеличилось до 1400. Локальные объекты групповой политики существовали независимо от того, входит ли компьютер в состав домена, рабочей группы или вовсе не принадлежит к сетевой среде. Все это объекты хранились в папке %SystemRoot%\System32\GroupPolicy. Политики распространялись только на тот компьютер, где хранятся сами GPO. В том случае, если компьютер не принадлежал к домену, локальная политика использовалась только для настройки конфигурации локального компьютера. Но если он входил в состав домена ActiveDirectory, то параметры, привязанные к инфраструктурной единице домена (домен, лес, сайт) заменяли параметры локального объекта групповой политики.

Операционные системы WindowsVista и WindowsServer 2008 уже поддерживают около 2500 настроек групповых политик. Новые категории управления политиками теперь уже обеспечивают управление питанием, возможность блокировки установки устройств, улучшенные параметры безопасности, расширение настроек InternetExplorer, а также возможность делегировать пользователям право устанавливать драйверы принтеров. В этих операционных системах было создано расширение для формата шаблонов политик. У форматов adm был значительный недостаток - для реализации локализации групповых политик нужно было создавать отдельный adm-файл для каждого языка. Теперь административные шаблоны представляют собой пару XML-файлов - *.admx файл, который определяет изменения в реестре, а также adml файл, который отвечает за языковые настройки указанной политики. Несмотря на эти изменения, в одной системе могут сосуществовать как adm, так и admx/adml шаблоны без всяких проблем. В операционной системе WindowsServer 2008 можно создавать стартовые объекты групповой политики. Использование стартового объекта групповой политики позволяет хранить набор параметров административных шаблонов политик в одном объекте и включать эти параметры в новые объекты групповой политики. Также для каждого объекта групповых политик появились возможности добавления комментариев, а сведения о подключенных сетях обеспечивают улучшение отклика групповой политики на изменение сетевых условий.

В операционных системах Windows 7 и WindowsServer 2008 R2 уже насчитывается около 3200 настроек групповых политик.

3.3. *Оснастка «Редактор локальной групповой политики»*

Объекты групповых политик делятся на две категории:

1. «Доменные объекты групповых политик», которые используются для централизованного управления конфигурацией компьютеров и пользователей, входящих в состав домена ActiveDirectory. Эти объекты хранятся только на контроллере домена.
2. «Локальные объекты групповых политик», которые позволяют настраивать конфигурацию локального компьютера, а также всех пользователей, созданных на этом компьютере. Эти объекты хранятся только в локальной системе. Локальные объекты групповых политик могут применяться, даже если компьютер входит в состав домена. *Для управления локальными объектами групповых политик в операционных системах Windows используется оснастка консоли управления* ***«Редактор локальной групповой политики».*** При помощи данной оснастки вы можете настраивать большинство системных компонентов и приложений.

В оснастке редактора локальных объектов групповой политики присутствуют два основных узла:

3.3.1. Узел ***«Конфигурация компьютера».***

Узел ***«Конфигурация компьютера»*** предназначен для настройки параметров компьютера. В этом узле расположены параметры, которые применяются к компьютеру, невзирая на то, под какой учетной записью пользователь вошел в систему. Эти параметры применяются при запуске операционной системы и обновляются в фоновом режиме каждые 90-120 минут.Узел ***«Конфигурация компьютера»*** содержит ***три дочерних узла***, при помощи которых настраиваются все параметры локальных объектов групповых политик: *«Конфигурация программ», «Конфигурация Windows», «Административные шаблоны».*

3.3.2. Узел ***«Конфигурация пользователя»***

Узел ***«Конфигурация пользователя»***предназначен для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему. Так же, как и параметры, расположенные в узле конфигурации компьютера, параметры, расположенные в узле конфигурации пользователя обновляются в фоновом режиме каждые 90-120 минут.Узел ***«Конфигурация пользователя»*** также содержит ***три дочерних узла***, при помощи которых настраиваются все параметры локальных объектов групповых политик:*«Конфигурация программ», «Конфигурация Windows», «Административные шаблоны».*

В дочернем узле «***Конфигурация программ»*** расположено только одно расширение клиентской стороны «*Установка программ»,* благодаря которому, вы можете указать определенную процедуру установки программного обеспечения. Расширения клиентской стороны (Client-Side-Extension, CSE) преобразовывает указанные параметры в объект групповой политики и вносит изменения в конфигурацию пользователя или компьютера. Создавать объекты групповой политики для развертывания

программного обеспечения можно только в операционной системе WindowsServer 2008/2008R2.

Дочерний узел ***«Конфигурация Windows»*** в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики. В нем вы можете найти несколько опций безопасности «Политика разрешения имен», «Сценарии», «Развернутые принтеры», «Параметры безопасности». Особый интерес представляет опция «Параметры безопасности». Эта опция позволяет настраивать политики безопасности средствами GPO. В этой опции для конфигурации безопасности компьютера доступны следующие настройки политик:

- *Политики учетных записей*(позволяют устанавливать политику паролей и блокировки учетных записей).
- *Локальные политики*(отвечают за политику аудита, параметры безопасности и назначения прав пользователя).
- *Политики открытого ключа*(позволяют: настраивать компьютеры на автоматическую отправку запросов в центр сертификации предприятия и установку выдаваемых сертификатов;создавать и распространять список доверия сертификатов (CTL);добавлять агенты восстановления шифрованных данных и изменение параметров политики восстановления шифрованных данных; добавлять агенты восстановления данных шифрования диска BitLocker).
- *Политики ограниченного использования программ*(позволяют осуществлять идентификацию программ и управлять возможностью их выполнения на локальном компьютере, в подразделении, домене и узле).
- *Политики управления приложениями*(отвечают за создание и управления правилами и свойствами функционала AppLocker, который позволяет управлять установкой приложений и сценариев).
- *Политики IP-безопасности на «Локальный компьютер»*(позволяют создавать политику IP-безопасности локального компьютера и управлять списками IP–фильтров).

Дочерний узел ***«Административные шаблоны»*** является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows. Каждому параметру политики административных шаблонов соответствует определенный параметр системного реестра.

Политики в дочернем узле «***Административные шаблоны»*** узла *«Конфигурация компьютера»* изменяют значения реестра в ключе HKEY_LOCAL_MACHINE (или просто HKLM), а политики в дочернем узле «***Административные шаблоны»*** узла *«Конфигурация пользователя»* - HKEY_CURRENT_USER (HKCU). В некоторых источниках административные шаблоны могут называться политиками на основе реестра. В рамках этой работы должен быть рассмотрен дочерний узел «***Административные шаблоны»*** для локального компьютера. О

применении настроек административных шаблонов для нескольких компьютеров или пользователей, входящих в домен, в данной работе не обсуждается.Для системных администраторов дочерний узел «***Административные шаблоны»*** предоставляет возможности динамического управления операционной системой. Несмотря на то, что администратору понадобится немало времени на настройку этого узла, все изменения, примененные при помощи групповых политик, невозможно будет изменить средствами пользовательского интерфейса.

4. Последовательность выполненияработы

4.1. ***Установить макет варианта лабораторной работы на диске С (VirtualBox).***

4.2. ***Выбрать оснастку«Редактора локальной групповой политики»***

Открыть данную оснастку можно несколькими способами:

1. Нажмите на кнопку «Пуск» для открытия меню, в поле поиска введите «Редактор локальной групповой политики» и откройте приложение в найденных результатах;

2. Воспользуйтесь комбинацией клавиш «+R» для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите *gpedit.msc* и нажмите на кнопку «ОК»;

3. Откройте «Консоль управления ММС». Для этого нажмите на кнопку «Пуск», в поле поиска введите *mmc*, а затем нажмите на кнопку «Enter». Откроется пустая консоль ММС. В меню «Консоль» выберите команду «Добавить или удалить оснастку» или воспользуйтесь комбинацией клавиш Ctrl+M. В диалоге «Добавление и удаление оснасток» выберите оснастку «Редактор объектов групповой политики» и нажмите на кнопку «Добавить». В появившемся диалоге «Выбор объекта групповой политики» нажмите на кнопку «Обзор» для выбора компьютера или нажмите на кнопку «Готово» (по умолчанию установлен объект «Локальный компьютер»). В диалоге «Добавление или удаление оснасток» нажмите на кнопку «ОК».

4.3. ***Провести настройки политик безопасности***

Провести настройки опций и политик безопасности дочерних узлов ***«Конфигурация программ»,«Конфигурация Windows»*** и ***«Административные шаблоны»*** для узлов ***«Конфигурация компьютера»*** и ***«Конфигурация пользователя».*** При настройке опции «Сценарий» использовать сценарии на языках программирования и сценарии PowerShell (в пункте контекстного меню для свойства «Автозагрузка» выбрать вкладку «Сценарии PowerShell».

4.3.1. Узел «Конфигурация компьютера»

4.3.1.1. Настроить дочерний узел «Конфигурация программ».

4.3.1.2. Настроить дочерний узел «Конфигурация Windows» (опции: *«Сценарии»*;*«Параметры безопасности»;*

4.3.1.3. Настроить дочерний узел «Административные шаблоны» (опции: *«Компоненты Windows»; «Система»; «Сеть»; «Совместимость приложений».*

4.3.2. Узел «Конфигурация пользователя».

4.3.2.1. Настроить дочерний узел «Конфигурация программ».

4.3.2.2. Настроить дочерний узел «Конфигурация Windows» (опции: *«Сценарии»;«Параметры безопасности»;«Настройки InternetExplorer»; «Политика разрешения имен»; «Развернутые принтеры»;* «Диспетчер вложений»;«Служба терминалов»;

4.3.2.3. Настроить дочерний узел «Административные шаблоны»(опции: *«Компоненты Windows»*; *«Панель задач и меню «Пуск»; «Общие папки»; «Панель управления»; «Рабочий стол»;«Сеть»; «Система»* (Доступ портативных носителей информации)*; «Все параметры»*.

5. Методические указания к выполнению работы

5.1. *Выбор пути к настройке групповых политик безопасности*

Перейти к настройке групповых политик безопасности, можно несколькими способами, в том числе через использование системного окна «Выполнить» и через консоль управления оснастками. Рассмотрим их по очереди и определим, который из способов удобнее – им и будем пользоваться в дальнейшем выполнении лабораторной работы.

5.1.1. Использование системного окна «Выполнить»

Используя комбинацию клавиш **WIN+R** вызовем диалог **«Выполнить»**(рис. 5.1):

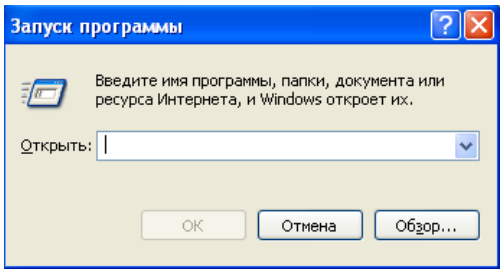


Рис. 4.1. Диалог «Выполнить»

В диалоговом окне **«Выполнить»**, в поле **«Открыть»** ввести*gpedit.msc*(рис. 5.2)*:*

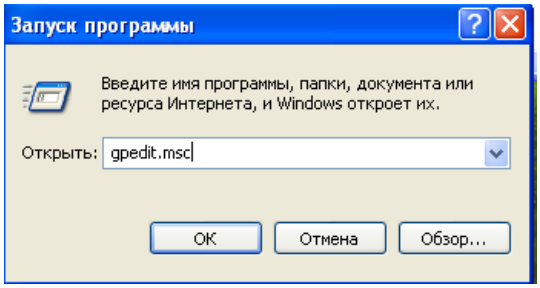


Рис. 5.2. Системное окно «Выполнить» с введенной командой вызова приложения «Групповая политика»

После нажатия на кнопку **«ОК»** откроется искомое приложение (рис.5.3):

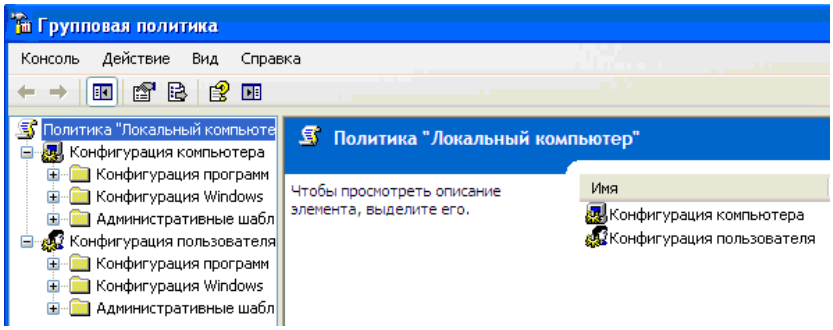


Рис. 5.3. Приложение «Групповая политика», открытое с помощью использования системного окна «Выполнить»

5.1.2. *Использование консоли управления оснастками MMC*

Используя комбинацию клавиш **WIN+R** вызовем диалог **«Выполнить»** и ввести в поле поиска *mmc*(рис. 5.4.):

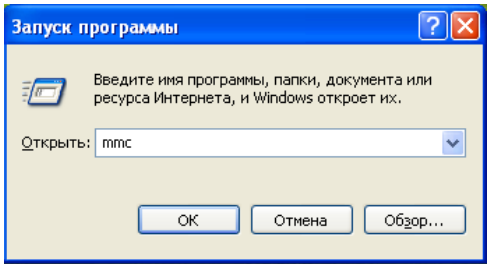


Рис. 5.4. Системное окно «Выполнить» с введенной командой вызова консоли управления оснастками

После нажатия на кнопку **«ОК»** откроется пустая консоль MMC (рис.5.5):

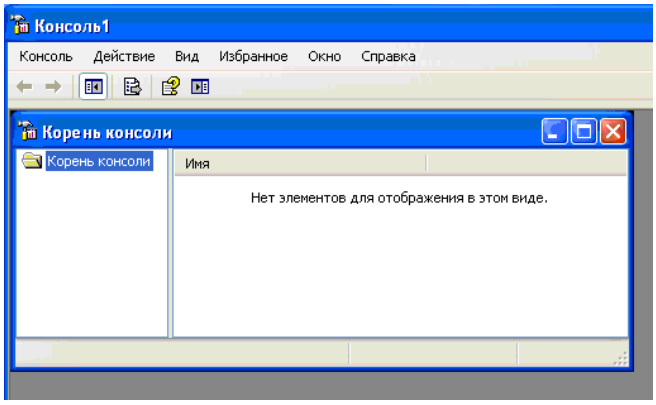


Рис.5. 5. Пустая консоль MMC

В меню **«Консоль»** выбрать **«Добавить или удалить оснастку»** для открытия диалога **«Добавление и удаление оснасток»**(рис.5.6)**:**

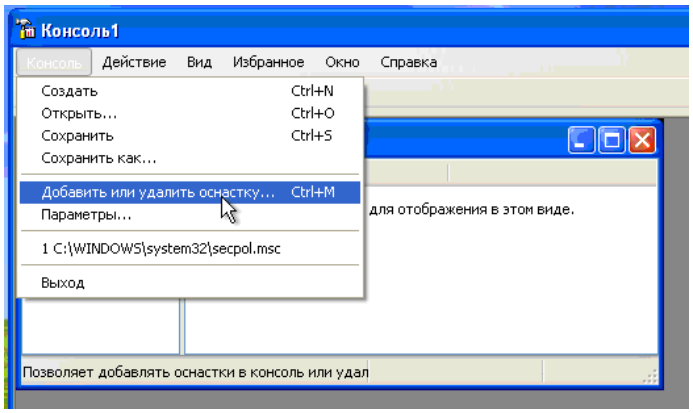


Рис. 5.6. Добавление новой оснастки

Из предложенных вариантов диалогового окна выбрать **«Редактор объекта групповой политики»** и нажать на кнопку **«Добавить»**(рис.5.7):

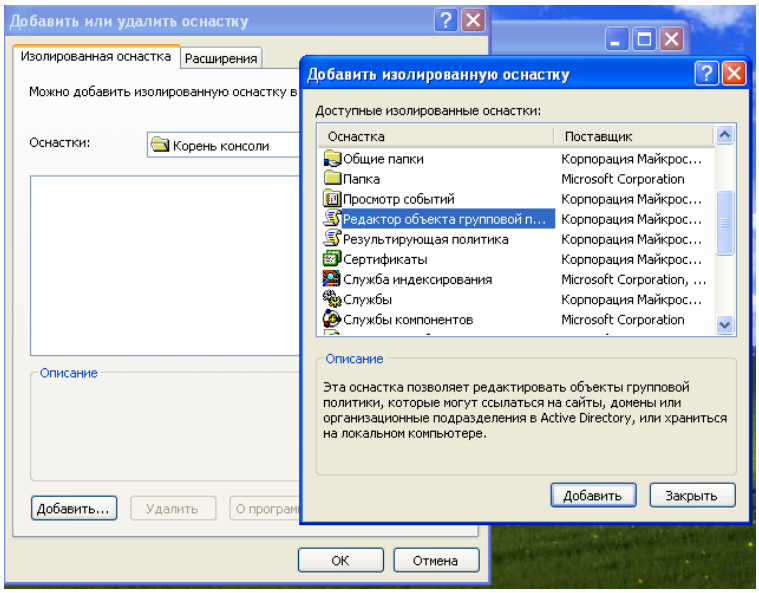


Рис. 5.7. Выбор«Редактор объекта групповой политики»

В появившемся диалоге **«Выбор объекта групповой политики»** нужно выбрать объект **«Локальный компьютер»**(рис.5.8):

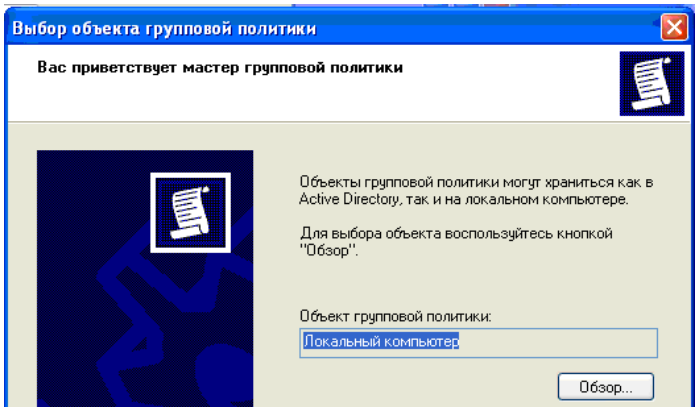


Рис. 5.8. Выбор объекта групповой политики

После нажатия в диалоге **«Добавление или удаление оснасток»** кнопки **«ОК»** откроется искомое приложение (рис.5.9):

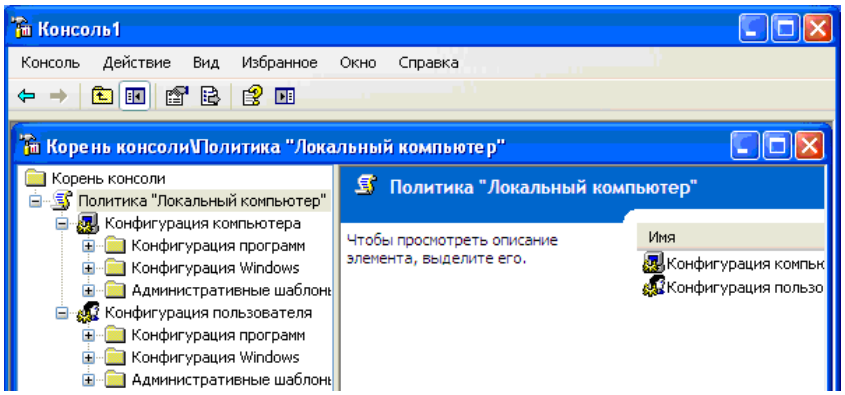


Рис. 5.9. Приложение «Групповая политика», открытое с помощью использования консоли управления оснастками MMC

Вывод по пункту: очевидно, что все три способа эквиваленты, поскольку приводят к одному и тому же результату: к открытию приложения **«Групповая политика»**. Однако, исходя из вышеприведенных последовательностей действий, необходимых для реализации каждого способа, *проще всего вызвать искомое приложение через системное окно* ***«Выполнить»***, что соответствует первому способу. Он и будет использоваться в дальнейшем выполнении лабораторной работы.

5.2. *Настройка групповой политики*

Объекты групповых политик делятся на две категории:

- **«Доменные объекты групповых политик»**, которые используются для централизованного управления конфигурацией компьютеров и пользователей, входящих в состав домена ActiveDirectory. Эти объекты хранятся только на контроллере домена;

- **«Локальные объекты групповых политик»**, которые позволяют настраивать конфигурацию локального компьютера, а также всех пользователей, созданных на этом компьютере. Эти объекты хранятся только в локальной системе. Локальные объекты групповых политик могут применяться, даже если компьютер входит в состав домена.

Для управления локальными объектами групповых политик в операционных системах Windows и используется оснастка консоли управления **«Групповая политика»**. При помощи данной оснастки вы можете настраивать большинство системных компонентов и приложений.

Заметим, что для успешного выполнения настроек политик, учетная запись, под которой выполняются данные действия, должна входить в локальную группу **«Администраторы»** на локальном компьютере. Проверим, так ли это для текущего АРМ:

Откроем **«Учетные записи пользователей»**, перейдя по адресу: *Пуск → Панель управления → Учетные записи пользователей* и проверим, какие пользователи вообще существует на данном АРМ (рис.5.10):

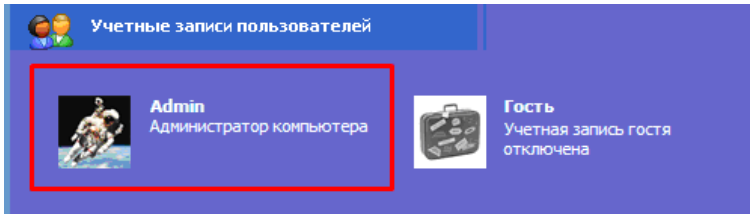


Рис. 5.10. Учетные записи пользователей

Очевидно, что текущая учетная запись – Admin – является единственной рабочей учетной записью на АРМ, а также является администратором компьютера. Следовательно, для данной учетной записи возможно успешное выполнение настроек политик.

В оснастке редактора локальных объектов групповой политики присутствуют два основных узла (рис. 5.11):

Узел **«Конфигурация *компьютера*»**, который предназначен для настройки параметров компьютера. В этом узле расположены параметры, которые применяются к компьютеру, невзирая на то, под какой учетной записью пользователь вошел в систему. Эти параметры применяются при запуске операционной системы и обновляются в фоновом режиме каждые 90-120 минут. Содержит три дочерних узла, при помощи которых настраиваются все параметры локальных объектов групповых политик (рис.5.11): **«Конфигурация программ»**, **«Конфигурация Windows»**, **«Административные шаблоны»**.

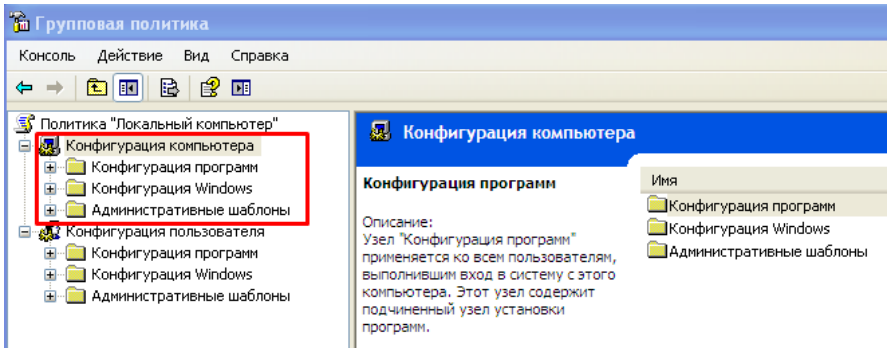


Рис. 5.11. Содержимое узла «Конфигурация компьютера» приложения «Групповая политика»

«Конфигурация *пользователя*», который предназначен для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему. Так же, как и параметры, расположенные в узле конфигурации компьютера, параметры, расположенные в узле конфигурации пользователя обновляются в фоновом режиме каждые 90-120 минут. Также содержит три дочерних узла, при помощи которых настраиваются все параметры локальных объектов групповых политик (рис.5.12): **«Конфигурация программ»**, **«Конфигурация Windows»**, **«Административные шаблоны»**.

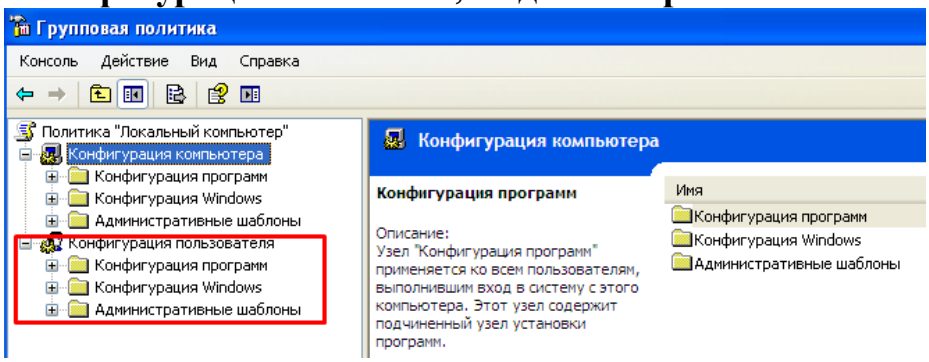


Рис. 5.12. Содержимое узла «Конфигурация пользователя» приложения «Групповая политика»

*5.2.1. Настройка узла**«Конфигурации компьютера»***

Для выполнения данного пункта задания требуется настроить опции и политики безопасности дочерних узлов **«Конфигурация Windows»** и **«Административные шаблоны»** для узла **«Конфигурация компьютера»**.

Политика паролей зависит от того, для каких целей предполагается использовать АРМ: она будет серьезнее или слабее. Предположим, что АРМ, о котором речь пойдет далее, находится в закрытом контуре некоторого предприятия, и на нем происходит обработка каких-то данных, касающихся работы предприятия и собранных в открытом контуре. Раз в неделю системный администратор проверяет данное АРМ, просматривает журналы и логии работы пользователя за прошедшую неделю и, при необходимости, вносит корректировки.

Приступим к выполнению задания с учетом вышеуказанных параметров.

5.2.1.1. Настройка дочернего узла «Конфигурация Windows» в **«Конфигурации компьютера»**

Открыть оснастку **«Конфигурация Windows»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел«Конфигурация Windows»*. Ниже можно увидеть содержимое узла **«Конфигурация Windows»** до внесения изменений (рис.5.13):

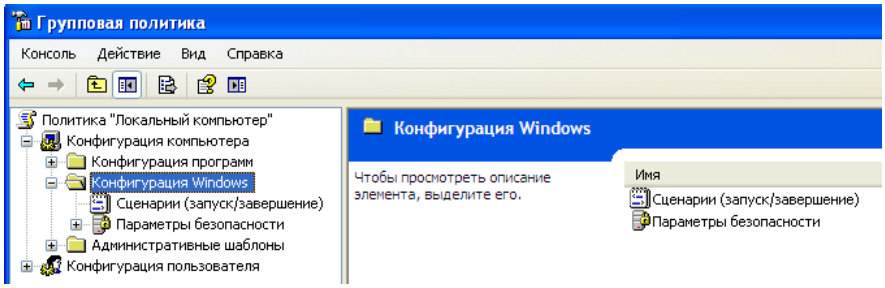


Рис. 5.13. Содержимое узла «Конфигурация Windows» до внесения изменений

Перейдем к настройке узла **«Сценарии»** в дочернем узле **«Конфигурация Windows»** приложения **«Групповые политики»**. Для этого откроем оснастку **«Сценарии»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел«Конфигурация Windows» → узел «Сценарии»*.

Групповые политики Windows позволяют запускать различные файлы скриптов при загрузке/ завершении работы компьютера, входе/выходе пользователя. С помощью «Групповых политик» можно исполнять на компьютерах домена не только классические файлы скриптов (.bat, .cmd, ,vbs), но скрипты PowerShell (.ps1).

WindowsPowershell - оснастка командной строки и скриптовый язык для различной автоматизации задач и администрирования в Windows. Скрипты Windows направлены на автоматизацию рабочего процесса.

Поскольку АРМ расположено в «закрытом» контуре, напишем скрипт с названием **«GetAllFiles.ps1»** на языке PowerShell, который будетвыводить на экран и в файл **C:\CountFiles.csv** информацию о том, сколько содержит файлов каждая папка и подпапки в директории **C:**, а также размер этих папок и подпапок. **CountFiles.csv** файл можно импортировать в **MicrosoftExcel** или в другое удобное приложения для работы с таблицами, и отсортировать столбцы файла по возрастанию или спаданию.

Этот скрипт будет запускаться при входе пользователя в систему и при выходе из нее: собранная за день информация дает представление о том, чем занимался пользователь на АРМ (и при необходимости сообщает системному администратору о подозрительной деятельности пользователя). Сравнение

количества файлов при выходе из системы «сегодня» и количества файлов на входе в систему «завтра» позволяет проверить, не были ли внесены какие-то изменения в файловую систему за время отсутствия пользователя, т.е. не получил ли некий злоумышленник доступа к АРМ и не внес ли в него изменения.

Содержимое скрипта **«GetAllFiles.ps1»**, расположенного по адресу **«C:\Scripts»**(рис.5.14)**:**

```
$source="C:"
Get-ChildItem $source -recurse -force | where {$_.psIscontainer} | foreach {
    $count = Get-ChildItem $_.fullname -recurse | where {$_.length} | Measure-Object -property length -Sum
    Write-Host($_.FullName)
    $FilesSize = '{0:F}' -f ((($count.Sum)/1024)/1024)
    Write-Host("Files: " + $count.count )
    Write-Host("Size: " + $FilesSize + " MB")
    '"' + $_.FullName + '",' + $count.count + ',' + $FilesSize + '' | Out-File C:\CountFiles.csv -Append
}
```

Рис. 5.14. Содержимое скрипта, считающего количество файлов в папках директории C:

Добавим скрипт **«GetAllFiles.ps1»** в сценарии автозгрузки (рис. 5.15):

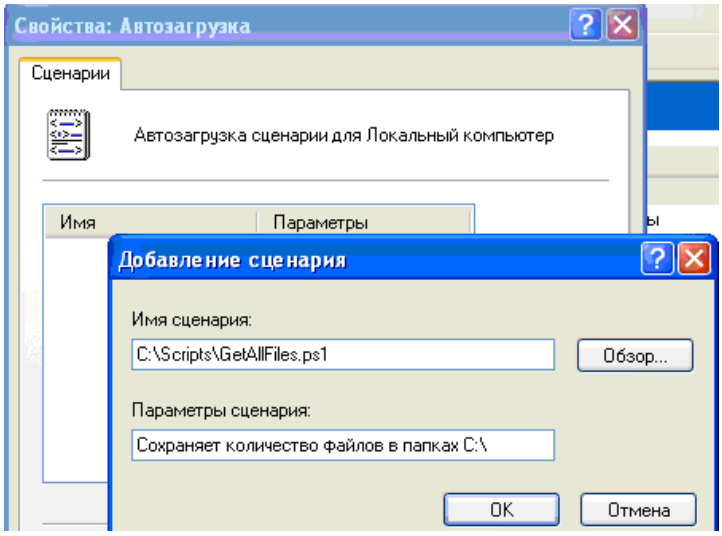


Рис. 5.15. Добавление скрипта в автозагруку

Очевидно, что теперь при запуске системы будет выполняться скрипт, который посчитает количество файлов на диске «C:\» (рис.5.16):

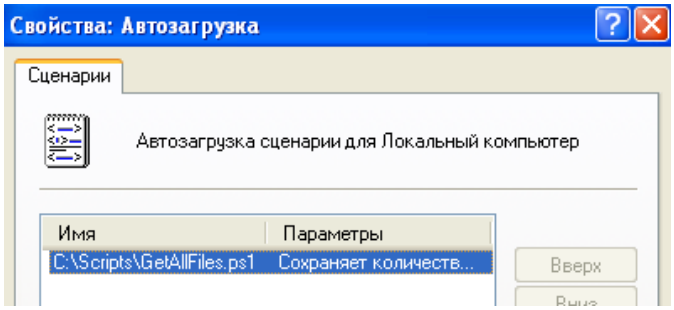


Рис. 5.16. Свойство «Автозагрузка» после внесения изменений

Добавим этот же скрипт **«GetAllFiles.ps1»** в сценарии автозапуска (рис.5.17):

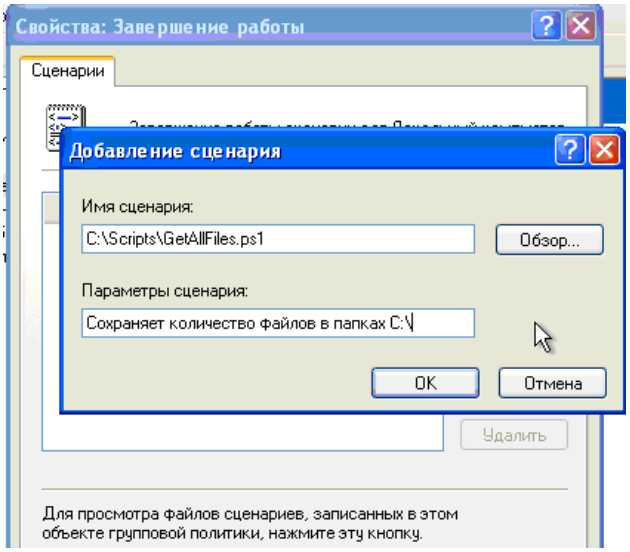


Рис. 5.17. Добавление скрипта в завершение работы

Очевидно, что теперь при завершении работы системы будет выполняться скрипт, который посчитает количество файлов на диске «C:\» (рис. 5.18):

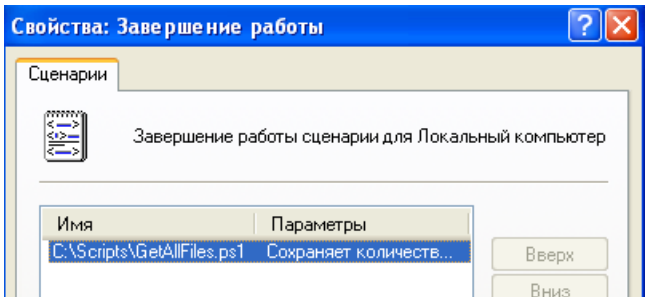


Рис. 5.18. Свойство «Завершение работы» после внесения изменений

«Сценарии» политики **«Конфигурация Windows»** успешно настроены.

Промежуточный вывод: в процессе выполнения данного этапа задания были настроены сценарии, которые будут выполняться при автозапуске и завершении работы Windows. Специально для этого и при учете места расположения АРМ был написан скрипт **«GetAllFiles.ps1»**, который занимается подсчетом количества файлов и папок в директории C:\, и потом выводит эту информацию в специально созданный для этого файл **C:\CountFiles.csv.** Файл с отчетом о собранной информации имеет табличный формат, что упрощает удобство обработки данных впоследствии. Собранная за день информация дает представление о том, чем занимался пользователь на АРМ (и при необходимости сообщает системному администратору о подозрительной деятельности пользователя). Сравнение количества файлов при выходе из системы «сегодня» и количества файлов на входе в систему «завтра» позволяет проверить, не были ли внесены какие-то изменения в файловую систему за время отсутствия пользователя, т.е. не

получил ли некий злоумышленник доступа к АРМ и не внес ли в него изменения.

Перейдем к настройке опций**«Параметры безопасности»** в дочернем узле **«Конфигурация Windows»** приложения **«Групповые политики»**.

Дочерний узел **«Конфигурация Windows»** в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики. В нем вы можете найти несколько опций безопасности, но особый интерес представляет опция **«Параметры безопасности»**. Она позволяет настраивать политики безопасности средствами **«Групповой политики»**. В этой опции для конфигурации безопасности компьютера доступны следующие настройки политик:

- **Политики учетных записей**, которые позволяют устанавливать политику паролей и блокировки учетных записей.
- **Локальные политики** (можно не настраивать см. здесь ЛАБ№1), отвечающие за политику аудита, параметры безопасности и назначения прав пользователя.
- **Политики открытого ключа**, которые позволяют:

✓ настраивать компьютеры на автоматическую отправку запросов в центр сертификации предприятия и установку выдаваемых сертификатов;
✓ создавать и распространять список доверия сертификатов (CTL);
✓ добавлять агенты восстановления шифрованных данных и изменение параметров политики восстановления шифрованных данных;
✓ добавлять агенты восстановления данных шифрования диска BitLocker.

- **Политики ограниченного использования программ**, позволяющие осуществлять идентификацию программ и управлять возможностью их выполнения на локальном компьютере, в подразделении, домене и узле.
- **Политики управления приложениями**, отвечающие за создание и управления правилами и свойствами функционала AppLocker, который позволяет управлять установкой приложений и сценариев.
- **Политики IP-безопасности на «Локальный компьютер»**, которые позволяют создавать политику IP-безопасности локального компьютера и управлять списками IP-фильтров.

Напомним, что наше АРМ расположено в «закрытом» контуре ИС. Исходя из этого, настроим **«Политики учетных записей»**. Эта политика включает в себя настройку следующих узлов (рис. 5.19):

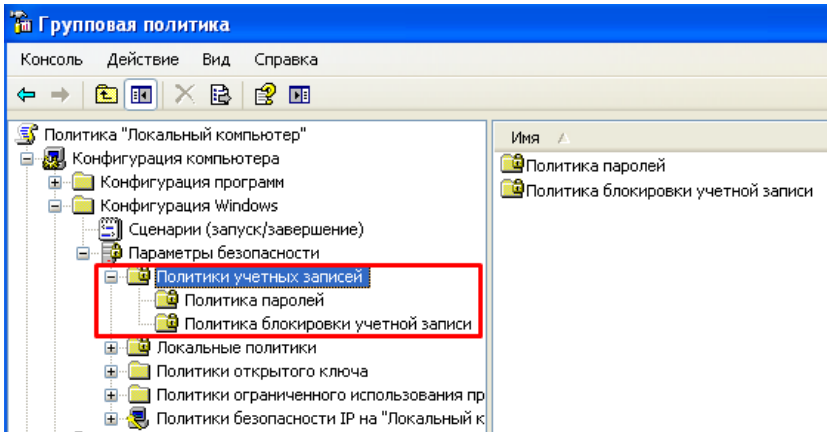


Рис. 5.19. Узлы политики «Политика учетных записей»

Откроем оснастку **«Политика паролей»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел«Конфигурация Windows»→ узел «Параметры безопасности» → узел «Политики учетных записей» → узел«Политики паролей»*.

«Политика учетных записей»аналогична локальным политикам безопасности. Поэтому используем ранее применяемые настройки для настройки политики **«Политика паролей»**(рис. 5.20):

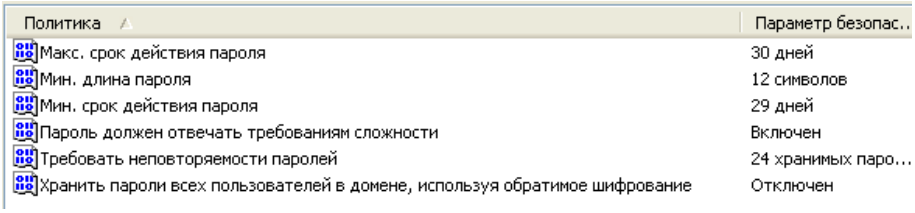


Рис. 5.20. Настройки политики «Политика паролей»

Поясним смысл настройки каждого пункта:

- **Максимальный срок действия пароля – 30 дней**

  Раз в неделю системный администратор домена, в который входит наше АРМ, проверяет состояние всех АРМ, чистит логи и исправляет ошибки. В соответствии с политикой предприятия, пароль меняется раз в месяц с привлечением административно ответственных лиц, поэтому значение параметра **«Макс. срок действия пароля»** должен быть установлен как **30**.

- **Минимальная длина пароля – 12 символов**

  Поскольку АРМ расположено в «закрытом» контуре, то установим для него длину пароля в параметре **«Мин. длина пароля»** не менее 12 символов (поскольку по рекомендациям безопасности оптимальное значение количества знаков для пароля серверов – от 10 до 12, наше АРМ не является сервером, но тем не менее усилим защиту).

- **Минимальный срок действия пароля – 29 дней**

  Устанавливается в соответствии с максимальным сроком действия пароля. Установим значение, равное **29**: получается, что пользователь АРМ

обязан использовать предоставленный ему системным администратором домена пароль весь месяц до тех пор, пока пароль не будет изменен в соответствии с политикой безопасности предприятия. Это, по сути, исключает возможность изменения пароля пользователем АРМ, что увеличивает защищенность самого АРМ.

- **Пароль должен отвечать требованиям сложности – Включен**

  Поскольку АРМ расположено в «закрытом» контуре, то на нем данный параметр обязательно должен быть в состоянии **«Включить»**, иначе нет смысла устанавливать пароль в 12 символов, когда он все равно будет уязвимым к взлому методом простого перебора.

- **Требовать неповторяемости паролей – 24 хранимых пароля**

  Поскольку АРМ расположено в «закрытом» контуре, а пароль к АРМ меняется каждый месяц, то разумно будет установить максимальное значение, которое только возможно для данного параметра. Это увеличит защищенность АРМ: если менять пароль каждый, то значение параметра **24** позволит хранить пароли за 2 года (!), что полностью исключает возможность использования старого пароля для получения несанкционированного доступа к АРМ.

- **Хранить пароли всех пользователей в домене, используя обратимое шифрование – Отключен**

  АРМ расположено в «закрытом» контуре, поэтому недопустимо хранить пароли в открытом виде: их может перехватить злоумышленник и без труда получить несанкционированный доступ к АРМ. Поэтому значение параметра установим**«Отключить».**

«Политика паролей» успешно настроена.

Промежуточный вывод: в процессе выполнения данного этапа задания была настроена «Политика паролей» при учете роли АРМ в предприятии. Даны пояснения применения настроек для каждого пункта политики. Данных настроек должно хватить для обеспечения безопасности АРМ в соответствии с предположением о цели АРМ, указанной в начале задания: данное АРМ представляет ценность для предприятия, системный администратор раз в неделю проверяет состояние АРМ, пароль к учетной записи АРМ меняется раз в месяц.

Откроем оснастку **«Политика блокировки учетных записей»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел«Конфигурация Windows»→ узел «Параметры безопасности» → узел «Политики учетных записей» → узел«Политики блокировки учетных записей»*.

Используем ранее применяемые настройки в локальной политике **«Политика блокировки учетных записей»** (рис. 5.21):

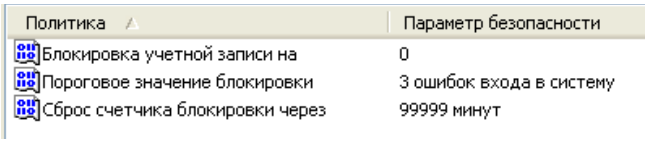


Рис. 5.21. Настройки политики «Политика блокировки учетных записей»

Поясним смысл настройки каждого пункта:

- **Блокировка учетной записи на – 0**
  Поскольку АРМ, которое рассматривается в данной лабораторной работе, расположено в «закрытом» контуре, то данный параметр разумно установить в значение **0**: в этом случае учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную. Эта мера предосторожности повысит защищенность АРМ: если будет превышено количество попыток входа (речь о которых идет далее), то этот случай уже вызывает подозрения – не действия ли это злоумышленника. Поэтому для сохранения безопасности АРМ учетная запись, для которой было превышено количество попыток входа, будет заблокирована до тех пор, пока с данной проблемой не разберется системный администратор.
- **Пороговое значение счетчика блокировки – 3 ошибки входа в систему**
  Поскольку АРМ расположено в «закрытом» контуре, установим значение данного параметра на **3** возможные попытки входа в учетную запись. Это рекомендуемое стандартное значение, и, с точки зрения безопасности, трех попыток хватит легальному пользователю, чтобы получить доступ к АРМ, а нелегальному – не хватит времени, чтобы подобрать правильный пароль до того, как учетная запись будет заблокирована.
- **Сброс счетчика блокировки через – 99999 минут**
  Поскольку для рассматриваемого АРМ значение параметра **«Продолжительность блокировки учетной записи»** было выбрано 0, то есть учетная запись будет заблокирована до тех пор, пока ее не разблокирует системный администратор, для данного параметра можно выбрать любое значение. Автоматическая разблокировка учетной записи не произойдет в любом случае, однако для дополнительной защищенности АРМ установим значение параметра **«Сброс счетчика блокировки»** на максимальное значение **99999**. Теперь в случае, если по какой-то причине предыдущая политика не вступит в силу, учетная запись все равно будет заблокирована на достаточно длительный срок, чтобы с причинами блокировки успел разобраться системный администратор и, при необходимости, предупредить действия злоумышленника.

«Политика блокировки учетных записей» успешно настроена.

«Параметры безопасности» политики **«Конфигурация Windows»** успешно настроены.

Промежуточный вывод: в процессе выполнения данного этапа задания была настроена «Политика блокировки учетных записей» при учете

роли АРМ в предприятии. Даны пояснения применения настроек для каждого пункта политики. Системный администратор один раз в неделю проверяет состояние АРМ.Пароль к учетной записи АРМ меняется один раз в месяц.

«Локальные политики», отвечающие за политику аудита, параметры безопасности и назначения прав пользователя, в соответствии с пояснениями к выполнению данной лабораторной работы настраиваются аналогично тому, как это было выполнено в «Лабораторной работе №1: Локальные политики безопасности АРМ», этапы настройки здесь приводиться не будут.

Откроем оснастку **«Политики безопасности IP на «Локальный компьютер»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел«Конфигурация Windows»→ узел «Параметры безопасности» → узел «Политики открытого ключа» → узел«Политики безопасности IP на «Локальный компьютер»*. Ниже можно увидеть содержимое политики после применения изменений (рис. 5.22):

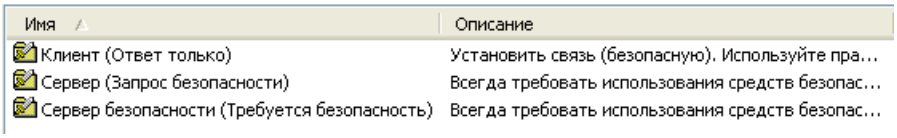


Рис. 5.22.Политики безопасности IP на «Локальный компьютер» после применения изменений

Поясним смысл настройки каждого пункта:

- **Клиент (Ответ только)**

Поскольку АРМ расположено в «закрытом» контуре, то в целях повышения безопасности пользователям не следует выходить в сеть Internet. Поэтому в соответствии с этой политикой запрещаются все запросы пользователя и разрешено только отправлять ответы (серверам предприятия). Также в целях повышения безопасности используется протокол проверки подлинности **Kerberos (**рис.5.23**)**:

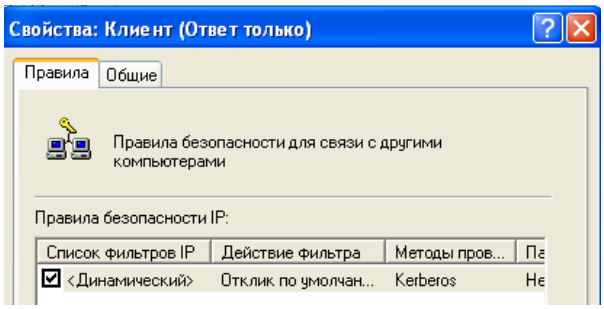


Рис. 5.23. Использование протокола Kerberos для проверки подлинности

- **Сервер (запрос безопасности)**

При обращении к серверу вначале передается запрос безопасности (рис. 5.24):

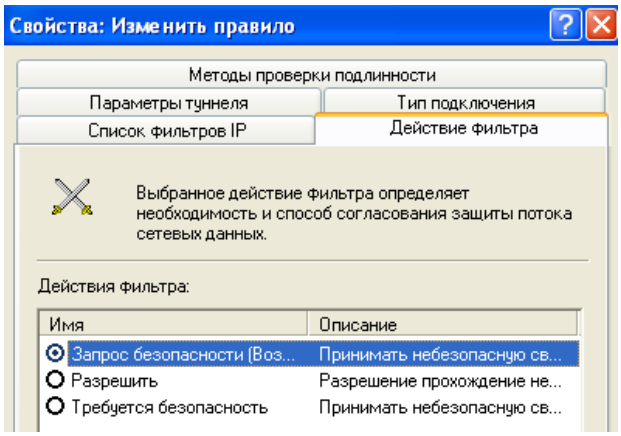


Рис. 5.24. Настройка использования запроса безопасности

Также в целях повышения безопасности для всех видов трафика требуется использование проверки подлинности с помощью протокола Kerberos (рис.5.25):

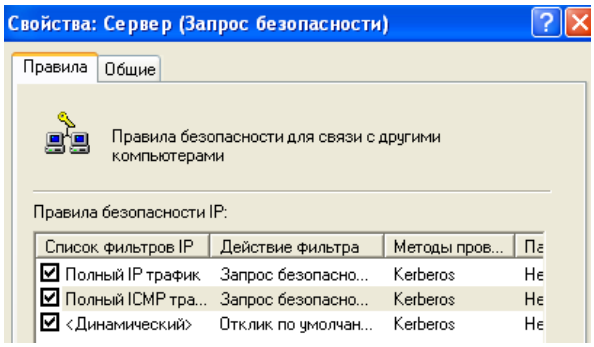


Рис. 5.245 Использование протокола Kerberos для проверки подлинности

- **Сервер безопасности (Требуется безопасность)**

Настраивается аналогично с пунктом «Сервер», с учетом всех требований к безопасности.

«Политики безопасности IP на «Локальный компьютер» успешно настроена.

Промежуточный вывод: в процессе выполнения данного этапа задания была настроена «Политики безопасности IP на «Локальный компьютер» при учете роли АРМ в предприятии. Даны пояснения применения настроек для каждого пункта политики. Данных настроек должно хватить для обеспечения безопасности АРМ в соответствии с предположением о цели АРМ, указанной в начале задания: данное АРМ представляет ценность для предприятия, системный администратор раз в неделю проверяет состояние АРМ, в целях безопасности пользователям АРМ запрещается выходить в сеть Internet.

5.2.1.2. Настройка дочернего узла «**Административные шаблоны**» в **«Конфигурации компьютера»**

Перейдем к настройке узла **«Административные шаблоны»** в дочернем узле **«Конфигурация Windows»** приложения **«Групповые политики»**.

Дочерний узел **«Административные шаблоны»** является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows. Каждому параметру политики административных шаблонов соответствует определенный параметр системного реестра.

Политики в дочернем узле «***Административные шаблоны»*** узла **«Конфигурация компьютера»** изменяют значения реестра в ключе HKEY_LOCAL_MACHINE (или просто HKLM). В рамках этой работы будет рассматриваться дочерний узел «***Административные шаблоны»*** для локального компьютера.

Поскольку политика «Административные шаблоны» включает в себя тысячи приложений и компонентов для гибкой настройки групповой политики безопасности под самые разные цели, нет смысла перечислять настройку всех компонентов. Вспомним, что рассматриваемое АРМ представляет ценность для предприятия, и в целях безопасности пользователям запрещается выходить в сеть Internet, разрешается отвечать на запросы серверов, а каждую неделю системный администратор проверяет состояние АРМ. Исходя из того, что АРМ расположено в «закрытом» контуре, настроим важные для безопасной его работы компоненты:

- **Запрет удаленного управления рабочим столом**

Откроем оснастку **«Запретить удаленное управление рабочим столом»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «NetMeeting» → узел«Запретить удаленное управление рабочим столом»*.

Поскольку предполагается, что рассматриваемая АРМ находится в защищенном контуре, то к ней могут подключаться только системный администратор и пользователь АРМ. Поэтому важно обязательно включить запрет на удаленное управление рабочим столом (рис.5.26):

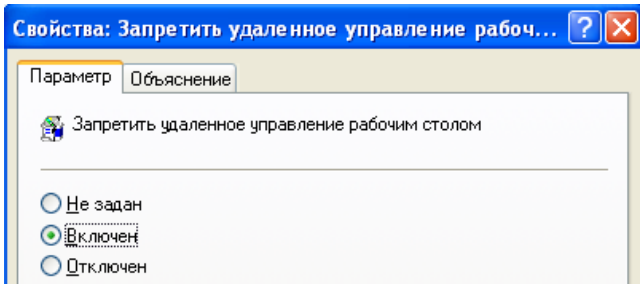


Рис. 5.26. Запрет удаленного управления рабочим столом

Этот же параметр регулируется из оснастки **«Разрешать удаленное подключение с использованием службы терминалов»**, расположенной по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Службы терминалов» → узел«Разрешать удаленное подключение с использованием службы терминалов»*. Запретим удаленное подключение, т.е. отключим разрешение на подключение (рис. 5.27):

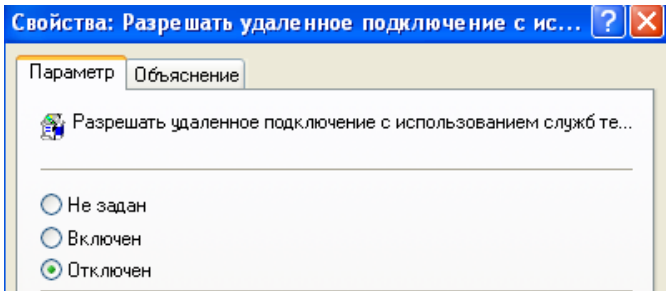


Рис. 5.27. Отключение разрешения на удаленное подключение

- **Выключить журнал событий справки приложения**

Откроем оснастку **«Выключить журнал событий справки приложения»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Совместимость приложений» → узел«Выключить журнал событий справки приложения»*.

Поскольку предполагается, что рассматриваемая АРМ не имеет доступа к интернету, то пользователь имеет возможность запускать только предустановленные программы и/или те, которые пользователь загружает непосредственно на АРМ с носителя. Последний случай представляет для системного администратора особый интерес: предполагается, что, в соответствии с политикой безопасности компании, личные носители информации, не прошедшие проверку, запрещены. Поэтому ведение журнала запуска приложений позволит отследить, из какого источника был запущен процесс, и отследить нарушителей (рис. 5.28).

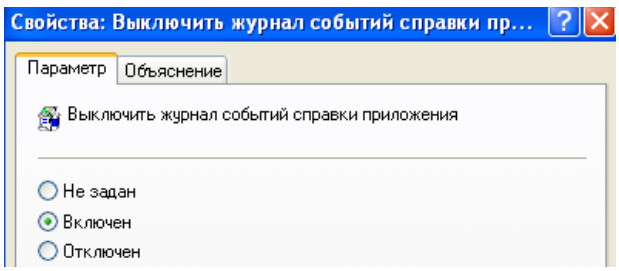


Рис. 5.28. Включение журнала событий справки приложений

- **Предотвращение доступа к 16-разрядным приложениям**

Откроем оснастку **«Предотвращение доступа к 16-разрядным приложениям»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел*

«Административные шаблоны» → узел «Совместимость приложений» → узел«Предотвращение доступа к 16-разрядным приложениям».

Современные операционные системы семейства Windows являются 32-х битными и 64-х битными. Рассматриваемая АРМ имеет операционную систему WindowsXP 32 бита, поэтому, с точки зрения логики, нет смысла разрешать запуск приложений меньшей разрядности: это может вызвать проблемы совместимости.

Кроме того, 16-ти битные приложения не безопасны, и, если вдруг пользователь запустит подобное приложение, злоумышленник теоретически может попытаться получить доступ к операционной системе жертвы через это уязвимое небезопасное приложение. Несмотря на то, что в нашем случае на АРМ недопустимо устанавливать и запускать сторонние приложения, следует предотвратить вероятность такой уязвимости (рис.5.29):

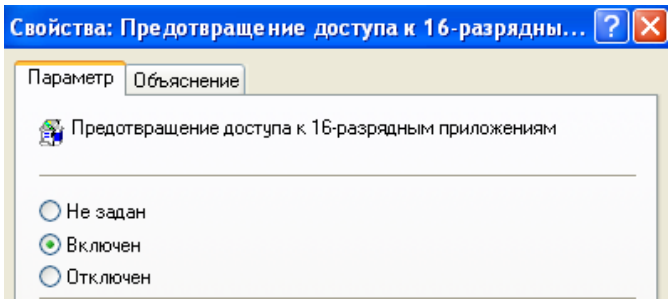


Рис. 5.29. Предотвращение доступа к 16-разрядным приложениям

- **Включение «Центра обеспечения безопасности»**

Откроем оснастку **«Включить центр обеспечения безопасности»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Центр обеспечения безопасности» → параметр«Включить центр обеспечения безопасности».*

При подключении АРМ к серверунеобходимо использовать все доступные механизмы обеспечения безопасности. В частности – **«Центр обеспечения безопасности»**(рис. 5.30):

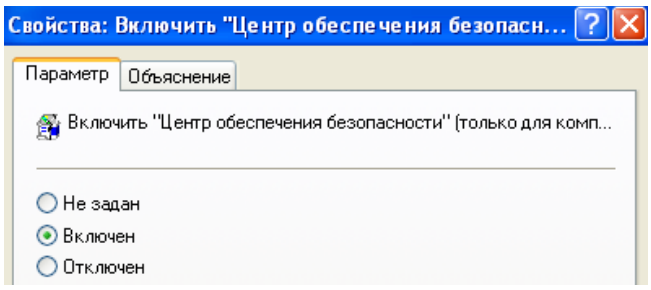


Рис. 5.30. Включение «Центра обеспечения безопасности»

- **Запрет удаления заданий**

Откроем оснастку **«Запретить удаление заданий»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел*

«Конфигурация компьютера» → узел «Административные шаблоны» → узел «Планировщик заданий» → параметр«Запретить удаление заданий».

Поскольку АРМ представляет ценность, для обеспечения ее безопасности системный администратор может устанавливать определенные задания: например, сбор статистики использования программ, журналирование событий и т.д. Эти задачи являются компонентом комплекса по обеспечению безопасности АРМ, и нельзя допустить, чтобы пользователь мог их изменять. Поэтому требуется установить запрет на удаление уже установленных для АРМ заданий (рис. 5.31):

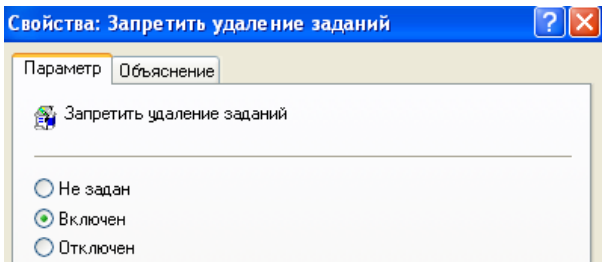


Рис. 5.31. Включение запрета удаления заданий

- **Удаление элемента «Безопасность Windows» из меню «Пуск»**

Откроем оснастку **«Удалить элемент «Безопасность Windows» из меню «Пуск»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Службы терминалов» → параметр«Удалить элемент «Безопасность Windows» из меню «Пуск».*

Рассматриваемая АРМ представляет ценность для предприятия, поэтому разумно будет убрать компонент «Безопасность Windows» из меню «Пуск», чтобы пользователь не имел доступа к настройкам безопасности в принципе (рис. 5.32):

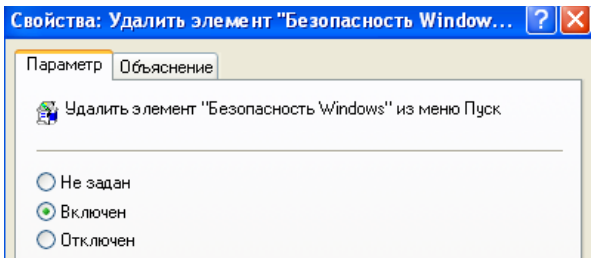


Рис. 5.32. Удаление элемента «Безопасность Windows» из отображения

- **Включение защищенного режима протокола оболочки**

Откроем оснастку **«Отключить защищенный режим протокола оболочки»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «Проводник» → параметр«Отключить защищенный режим протокола оболочки».*

Данный параметр регулирует возможность доступа к папкам и файлам, если используется защищенный режим, то приложения не могут запускать файлы, находящиеся под защитой. Для блокировки доступа пользователя к файлам и папкам, изменение которых может повредить работоспособности ОС и безопасности АРМ в частности, следует отключить этот параметр политики: в таком случае протокол оболочки используется в защищенном режиме, позволяя приложениям открывать только разрешенные папки (рис. 5.33).

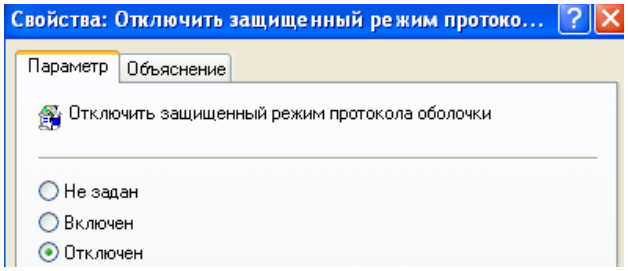


Рис. 5.33. Включение защищенного режима протокола оболочки

- **Ведение журнала запуска и установки приложений**

Откроем оснастку **«Ведение журнала»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел«Административные шаблоны» → узел «Установщик Windows» → параметр«Ведение журнала»*.

АРМ представляет ценность для предприятия, поэтому следует вести журнал всех процессов, генерируемых приложениями. Это позволит отследить, с чем и когда работает пользователь АРМ, а также определить, пытается ли он нарушить политику безопасности предприятия, устанавливая и запуская те приложения, которые не были предустановленны на его АРМ. Следовательно, необходимо включить **«Ведение журнала»**, а в параметрах записи указать все события (ошибки, состояние, действия и т.д.) – если системный администратор будет располагать всеми сведениями о происходящем на АРМ, ему будет проще регулировать события (рис. 5.34).

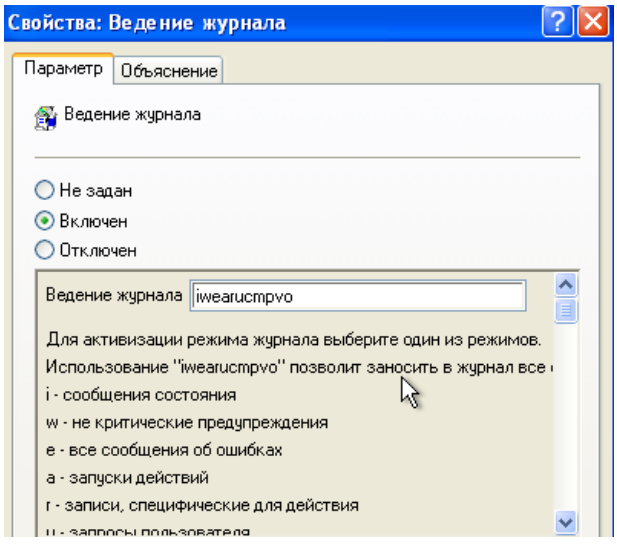


Рис. 5.34. Включение ведения журнала событий от приложений

- **Настройка автоматического обновления системы**

Откроем оснастку **«Настройка автоматического обновления»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел «Административные шаблоны» → узел «WindowsUpdate» → параметр«Настройка автоматического обновления»*.

Обновление системы важно: зачастую именно они повышают безопасность ОС, исправляя багги и ошибки, сделанные разработчиками ОС, и не применение обновлений, по сути, оставляет открытой уязвимость, которую пытаются исправить. Следовательно, этой уязвимостью может воспользоваться злоумышленник – значит, нужно своевременно обновлять ОС.

Однако, обновление ОС занимает время и ресурсы АРМ, во время обновления невозможно пользоваться АРМ – а значит, происходит потеря человекочасов и средств, которые можно было заработать за вынужденное время простоя. Поэтом необходимо настроить автоматическое обновление системы.

Предположим, что у пользователя, рассматриваемого АРМ 5-дневный 8-ми часовой рабочий день с 9:00 до 17:00, а пятница – сокращенный день, с 9:00 до 16:30. Значит, можно выбрать пятницу днем, когда разрешено автоматическое обновление системы: в 17:00 АРМ уже не будет нужно пользователю, т.е. все его ресурсы можно отдать обновлениям. В соответствии с этим настроим политику (рис. 5.35):

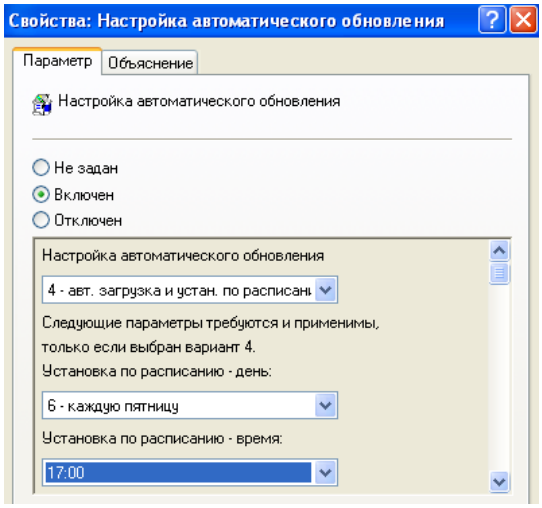


Рис. 5.35. Настройка автоматического обновления системы

«Административные шаблоны» оснастки **«Конфигурация компьютера»** успешно настроена.

Промежуточный вывод: в процессе выполнения данного этапа задания были настроены «Административные шаблоны» при учете роли АРМ в предприятии. Даны пояснения применения настроек для каждого

пункта политики. Данных настроек должно хватить для обеспечения безопасности АРМ в соответствии с предположением о цели АРМ, указанной в начале задания: данное АРМ представляет ценность для предприятия, системный администратор раз в неделю проверяет состояние АРМ, в целях безопасности пользователям АРМ запрещается выходить в сеть Internet, пользователям АРМ запрещается устанавливать приложения с личных носителей, не прошедших проверку. Также дополнительно были настроены параметры, которые позволят более гибко работать с ОС: например, настройки обновления Windows подобраны так, чтобы не мешать основной работе пользователя. Здесь же были заданы дополнительные настройки безопасности: включение «Центра управления безопасностью», запрет удаления системных заданий (таких как обновление, например), включение ведения журналов обо всех процессах, генерируемых приложениями, включен запрет на удаленный доступ к АРМ, включен защищенный режим протокола оболочки (который защитит системные файлы и закроет пользователю доступ к файлам, изменение которых повлияет на работоспособность АРМ).

Для системных администраторов дочерний узел "Административные шаблоны" предоставляет возможности динамического управления операционной системой. Несмотря на то, что администратору понадобится немало времени на настройку этого узла, все изменения, примененные при помощи групповых политик, невозможно будет изменить средствами пользовательского интерфейса.

На этом настройка узла **«Конфигурация компьютера»** закончена.

Вывод по пункту: в данной части лабораторной работе были настроены политики, относящиеся к узлу **«Конфигурация компьютера»,** предназначенному для настройки параметров компьютера. В этом узле расположены параметры, которые применяются к компьютеру, невзирая на то, под какой учетной записью пользователь вошел в систему.

Дочерний узел «Конфигурация программ» позволяет указать определенную процедуру установки программного обеспечения.

Дочерний узел «Конфигурация Windows» в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики.

Дочерний узел «Административные шаблоны» является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows.

В частности, в процессе выполнения данного задания были настроены:

- Конфигурация Windows, включая сценарии для автозагрузки и выключения АРМ и параметры безопасности Windows (политика паролей и блокировки учетных записей)
- Локальные политики и политики безопасности IP на «Локальный компьютер
- Административные шаблоны, включающие в себя компоненты для безопасной работы Windows

Настройка каждого параметра политик и журналов была обоснована.

Для каждого этапа настройки политик представлен промежуточный вывод.

5.2.2. *Настройка дочерних узлов «Конфигурации пользователя»*

Для выполнения данного пункта задания требуется настроить опции и политики безопасности дочерних узлов **«Конфигурация Windows»** и **«Административные шаблоны»** для узла **«Конфигурация компьютера»**.

Политика паролей зависит от того, для каких целей предполагается использовать АРМ: она будет серьезнее или слабее. Предположим, что АРМ, о котором речь пойдет далее, находится в закрытом контуре некоторого предприятия, и на нем происходит обработка каких-то данных, касающихся работы предприятия и собранных в открытом контуре. Раз в неделю системный администратор проверяет данное АРМ, просматривает журналы и логии работы пользователя за прошедшую неделю и, при необходимости, вносит корректировки.

Предполагается, что у пользователя, рассматриваемого АРМ 5-дневный 8-ми часовой рабочий день с 9:00 до 17:00, а пятница – сокращенный день, с 9:00 до 16:30. В конце каждого месяца все сотрудники составляют отчеты о проделанной работе.

АРМ имеет в домене IP-адрес 172.168.13.16, сервер, с которым связан АРМ – 172.168.13.1.

Приступим к выполнению задания с учетом вышеуказанных предположений.

5.2.2.1. Настройка дочернего узла «Конфигурация Windows» в **«Конфигурации пользователя»**

Откроем оснастку **«Конфигурация Windows»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел«Конфигурация Windows»*. Ниже можно увидеть содержимое узла **«Конфигурация Windows»** до внесения изменений (рис. 5.36):

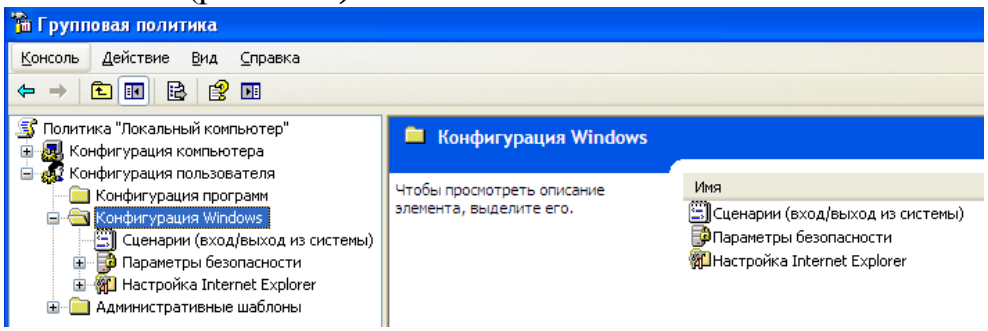


Рис. 5.36. Содержимое узла «Конфигурация Windows» до внесения изменений

Перейдем к настройке узла **«Сценарии»** в дочернем узле **«Конфигурация Windows»** приложения **«Групповые политики»**. Для этого откроем оснастку **«Сценарии»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация компьютера» → узел«Конфигурация пользователя» → узел «Сценарии»*.

Групповые политики Windows позволяют запускать различные файлы скриптов при загрузке/ завершении работы компьютера, входе/выходе пользователя. С помощью «Групповых политик» можно исполнять на компьютерах домена не только классические файлы скриптов (.bat, .cmd, ,vbs), но скрипты PowerShell (.ps1).

WindowsPowershell - оснастка командной строки и скриптовый язык для различной автоматизации задач и администрирования в Windows. Скрипты Windows направлены на автоматизацию рабочего процесса.

Поскольку текущее АРМ представляет ценность для компании, напишем скрипт с названием **«GetBackup.ps1»** на языке PowerShell, который будетделать бэкап системы при каждом выходе пользователя из системы. Ниже представлена часть содержимого скрипта, расположенного по адресу **«C:\Scripts»**(рис. 5.37):

```
$StartTimeHour = (Get-Date).Hour #Запоминаем когда запустилась задача
$Day_of_week = [int]((Get-Date).DayofWeek) #текущий день недели
if (($Day_of_week -eq 1)-or($Day_of_week -eq 3)-or($Day_of_week -eq 5))-and($StartTimeHour -eq 17)) {
#старт копирования если сейчас понедельник, среда, пятница и при этом 17 часов
 $StartTime = Get-Date -Format "yyyy.MM.dd HH:mm:ss" #время старта копирования
 $Free_Space_Start = Get-WMIObject Win32_LogicalDisk -Filter "DeviceID='C:'" | ForEach-Object {[math]::truncate($_.freespace / 1GB)}
 $Free_Space_Start_Bytes = Get-WMIObject Win32_LogicalDisk -Filter "DeviceID='D:'" | ForEach-Object {$_.freespace} #свободное место
 $log_file = "C:\Backups\log.txt" #лог файл скрипта, можно понять на каком этапе работа скрипта
 $date = "{0:yyyy-MM-dd}" -f (get-date) #текущая дата для имени папки
 $path = "\\172.168.13.1\BackupsFromPC16\" + $date + "\" #имя папки
 if (-not(Test-Path $path)) { #если папка не существует
 write-host "создаем папку: " + $path
 $result = New-Item -ItemType directory -Path $path #создаем папку }
 $time = "{0:yyyy-MM-dd HH:mm:ss}" -f (get-date)
 "################################################" | Out-File -Append $log_file -Encoding UTF8
 #копируем пользовательскую информацию
 $time = "{0:yyyy-MM-dd HH:mm:ss}" -f (get-date)
 $string = $time + " Start Copy \\172.168.13.16\Backups\Other"
 $string | Out-File -Append $log_file -Encoding UTF8
 & robocopy \\172.168.13.16\Backups\Other \\172.168.13.1\Backups\Other /e /log:"\\172.168.13.1\Backups\robocopy_log.txt"
 #копируем резервные копии Windows
 $path = $path + "WindowsImageBackup"
 $time = "{0:yyyy-MM-dd HH:mm:ss}" -f (get-date)
 $string = $time + " Start Copy \\172.16.13.16\Backups\WindowsImageBackup"
 $string | Out-File -Append $log_file -Encoding UTF8
 & robocopy \\172.168.13.16\Backups\WindowsImageBackup $path /e /log:"\\172.168.13.1\Backups\robocopy_log.txt"
 #запись в лог-файл окончания работы
 $time = "{0:yyyy-MM-dd HH:mm:ss}" -f (get-date)
 $string = $time + " Finish Backup"
 $string | Out-File -Append $log_file -Encoding UTF8
 "################################################" | Out-File -Append $log_file -Encoding UTF8
 ##формируем данные для письма
 $EndTime = Get-Date -Format "yyyy.MM.dd HH:mm:ss"
 $Free_Space_End = Get-WMIObject Win32_LogicalDisk -Filter "DeviceID='C:'" | ForEach-Object {[math]::truncate($_.freespace / 1GB)} #
 бекапа
 $Free_Space_End_Bytes = Get-WMIObject Win32_LogicalDisk -Filter "DeviceID='C:'" | ForEach-Object {$_.freespace} #свободное место до
 $backup_Size = $Free_Space_Start-$Free_Space_End
 $backup_Size_Bytes = $Free_Space_Start_Bytes-$Free_Space_End_Bytes
```

Рис. 5.37. Часть содержимого скрипта, создающего бэкап системы

Предполагается, что упользователя рассматриваемого АРМ 5-дневный 8-ми часовой рабочий день с 9:00 до 17:00, а пятница – сокращенный день, с 9:00 до 16:30. Если PowerShell скрипт запущен в определенное время и определенный день, а именно: в понедельник, среду и пятницу, на 17 часов вечера, – то он начинает копировать файлы из указанных папок:

- \\172.168.13.16\Backups\Other, которая предположительно содержит информацию, которую пользователь считает важной для своей работы и желает сделать для нее резервную копию;
- \\172.168.13.16\Backups\WindowsImageBackup, которая предположительно содержит все резервные копии системы.

Здесь 172.168.13.16 – присвоенный данному компьютеру IP-адрес в домене. Копирование происходит на сервер, расположенный по адресу 172.168.13.1 в аналогичные папки. Ход процесса записывается в лог файл.

После окончания работы на e-mail системного администратора присылается письмо, в котором указано: свободное место на локальных дисках (до старта и после окончания), объем резервной копии, время старта и окончания, средняя скорость копирования. После этого компьютер выключается (для резервного копирования он автоматически включается в соответствии с настройками BIOS, поэтому его следует повторно выключить).

Этот скрипт будет запускаться при выходе пользователя из системы, а запуск раз в два дня позволит обезопасить пользователя от потери информации и вызванных этим простоев. Также письмо, генерируемое скриптом и отправляемое системному администратору, позволит последнему быть в курсе происходящего на АРМ.

Добавим скрипт **«GetBackup.ps1»** в сценарии событий выхода из системы (рис. 5.38):

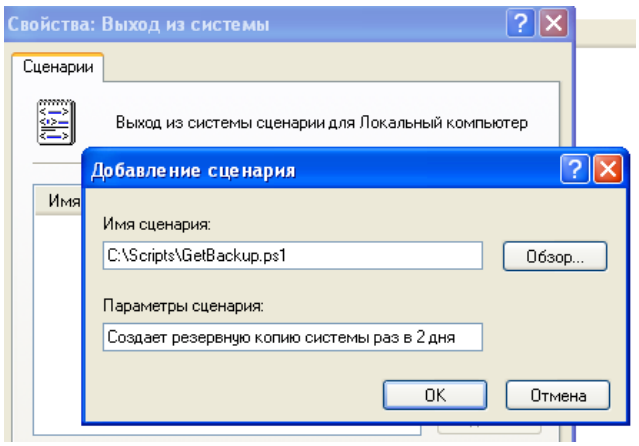


Рис. 5.38. Добавление скрипта к событиям выхода из системы

Теперь при каждом выходе пользователя из системы в понедельник, среду и пятницу в 17:00 часов вечера будет создаваться резервная копия всей важной информации.

Однако большое количество создаваемых каждую неделю копий (3 в неделю, 12 в месяц) может пагубно сказаться на памяти АРМ: в скрипте выделяет минимум 1 ГБ на создание копии, а в предприятии целесообразно экономить ресурсы. Поэтому напишем скрипт **«KillOldBackups.ps1»**, который будет запускаться при каждом входе пользователя в систему в понедельник в 9:00 утра. Этот скрипт будет сканировать папку **«C:\Backups»**, которая содержит резервные копии, создаваемые скриптом

«GetBackup.ps1», и смотреть на дату находящихся там резервных копий и удалять все бэкапы старше месяца.

Предполагается, что в конце каждого месяца все сотрудники составляют отчеты о проделанной работе, поэтому все резервные копии, дата создания которых старше текущей более чем на 1 месяц, уже не актуальны. Ниже представлено содержимое скрипта, расположенного по адресу **«C:\Scripts»**(рис. 5.39)**:**

```
if (($Day_of_week -eq 1)-and($StartTimeHour -eq 9))
$date = (Get-Date).AddMonths(-1)
Remove-Item "C:\Backups\*" -force -recurse
Get-ChildItem -Path C:\Backups\ | where {!$_.PSIsContainer} |
foreach {
    if ($_.LastWriteTime -lt $date) { Remove-Item $_ -whatif }
        }
}
```

Рис.5.39. Содержимое скрипта, удаляющего старые резервные копии backup

Этот скрипт будет запускаться при входе пользователя в систему и регулировать количество занимаемой уже не нужными резервными копиями памяти АРМ.

Добавим скрипт **«KillOldBackups.ps1»** в сценарии событий выхода из системы (рис. 5.40):

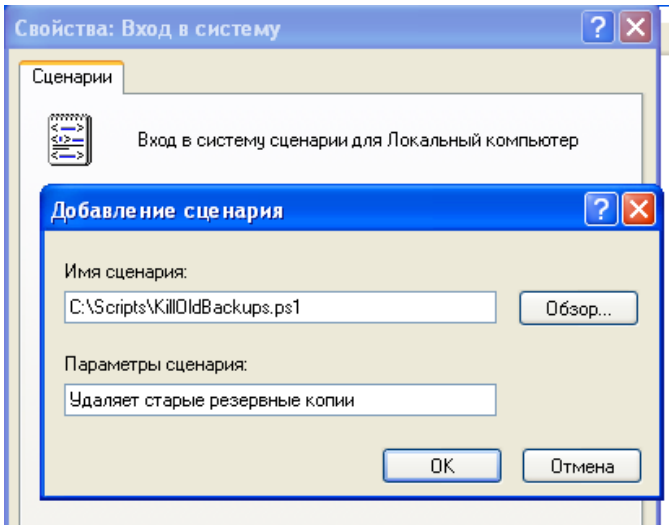


Рис. 5.40. Добавление скрипта к событиям входа в систему

Таким образом, специально для целей, выполняемых АРМ и в соответствии с рабочим графиком пользователя, были написаны два скрипта, выполняющих резервное копирование системы и содержащейся на ней важной информации и регулирующие количество занимаемой этими скриптами памяти.

«Сценарии» политики **«Конфигурация пользователя»** успешно настроены.

Промежуточный вывод: в процессе выполнения данного этапа задания были настроены сценарии, которые будут выполняться при входе и выходе пользователя АРМ в систему. Специально для этого и при учете роли АРМ и графика работы пользователя в предприятии были написаны скрипты **«GetBackup.ps1»**,который раз в два дня делает резервную копию системы и пользовательской информации, затем отправляет копию на сервер, создает лог выполнения копирования и отправляет лог в виде электронного письма на почту системного администратора, и**«KillOldBackups.ps1»**, который сканирует папку, содержащую резервные копии на АРМ, и удаляет все бэкапы старше 1 месяца. Первый скрипт позволяет сохранять всю важную для работы пользователя и предприятия информацию, предотвращать потерю данных и вызванный этим простой (который влечет убытки для предприятия), а также сообщать системному администратору информацию о процессе прохождения резервного копирования. Второй скрипт защищает АРМ от переполнения памяти.

Перейдем к настройке узла **«Настройки InternetExplorer»** в дочернем узле **«Конфигурация пользователя»** приложения **«Групповые политики»**.

Поскольку АРМ представляет ценность, то в интересах предприятия запретить пользователям доступ в интернет. Осуществим это с помощью **«Групповой политики»**, настроив параметры используемого прокси-сервера.

Для этого откроем оснастку **«Параметры прокси-сервера»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел«Конфигурация Windows»→ узел «Настройки InternetExplorer» → узел «Подключения»→ узел «Параметры прокси-сервера»*.

Для того, чтобы запретить пользователям доступ в интернет, достаточно указать в качестве обязательно используемого несуществующий IP-адрес прокси-сервера. Используем адрес «0.0.0.0», установим обязательным использование данного прокси-сервера для всех адресов, по которым пытаются обратиться пользователи.

Но, поскольку АРМ все еще требуется связь с сервером, который располагается предположительно по адресу 172.168.13.1, разрешим соединения с ним, записав его адрес в графу исключений.

С учетом вышеописанных параметров, настройки данной политики выглядят следующим образом (рис. 5.41):

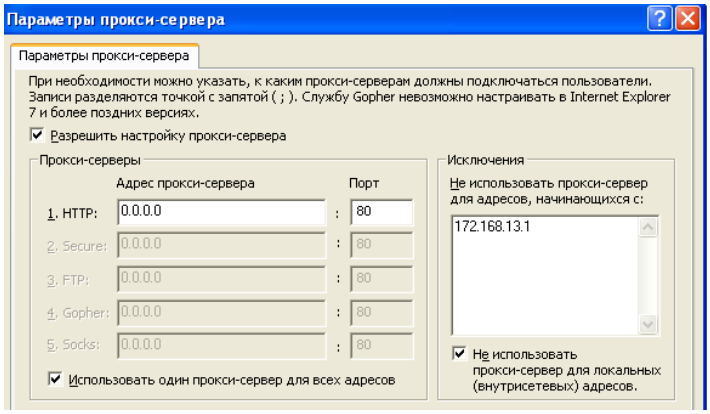


Рис. 5.41. Настройки прокси-сервера

«Настройки InternetExplorer» успешно настроена.

Промежуточный вывод: в процессе выполнения данного этапа задания были настроены «Настройки InternetExplorer» при учете роли АРМ в предприятии. Поскольку в целях безопасности следует запретить пользователям доступ в интернет, самой главной настройкой данной политики являются настройки прокси-сервера: было выставлено обязательное использование недействительного адреса прокси-сервера, что автоматически делает невозможным выход пользователя в сеть. Дальнейшие настройки политики «Настройки InternetExplorer» не представляют интереса, поскольку пользователь все равно не сможет получить доступ к сети интернет.

В качестве исключения указан адрес сервера, с которым связывается АРМ: это сделано для того, чтобы АРМ имел возможность отправлять резервные копии серверу.

5.2.2.2. Настройка дочернего узла «**Административные шаблоны**» в **«Конфигурации пользователя»**

Перейдем к настройке узла **«Административные шаблоны»** в дочернем узле **«Конфигурация пользователя»** приложения **«Групповые политики».**

Дочерний узел **«Административные шаблоны»** является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows. Каждому параметру политики административных шаблонов соответствует определенный параметр системного реестра.

Политики в дочернем узле **«Административные шаблоны»** узла **«Конфигурация пользователя»** изменяют значения реестра в ключе HKEY_CURRENT_USER (HKCU)

Для пользователя **«Административные шаблоны»** представляют собой настройки, связанные с интерфейсом АРМ (рис. 5.42):

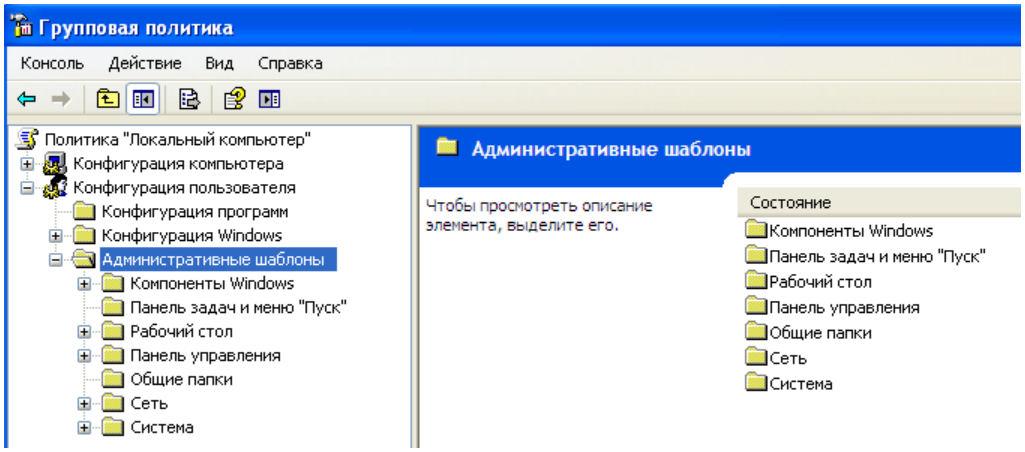


Рис. 5.42. Содержимое «Административных шаблонов» для «Конфигурации пользователя»

Поскольку политика «Административные шаблоны» включает в себя тысячи приложений и компонентов для гибкой настройки групповой политики безопасности под самые разные цели, нет смысла перечислять настройку всех компонентов. Следует определить, к каким компонентам пользователь АРМ, исходя из предназначения АРМ, может иметь доступ, а к каким – нет. Главным образом это касается доступа к настройкам АРМ, использование которых может нарушить работу АРМ (а, соответственно, и работу пользователя, что влечет за собой простой и финансовые убытки для предприятия).

- **Предотвращение доступа к 16-разрядным приложениям**

Откроем оснастку **«Предотвращение доступа к 16-разрядным приложениям»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows»→ узел «Совместимость приложений» → узел«Предотвращение доступа к 16-разрядным приложениям»*.

Современные операционные системы семейства Windows являются 32-х битными и 64-х битными. Рассматриваемая АРМ имеет операционную систему WindowsXP 32 бита, поэтому, с точки зрения логики, нет смысла разрешать запуск приложений меньшей разрядности: это может вызвать проблемы совместимости.

Кроме того, 16-ти битные приложения не безопасны, и, если вдруг пользователь запустит подобное приложение, злоумышленник теоретически может попытаться получить доступ к операционной системе жертвы через это уязвимое небезопасное приложение. Несмотря на то, что в нашем случае на АРМ недопустимо устанавливать и запускать сторонние приложения, следует предотвратить вероятность такой уязвимости (рис. 5.43):

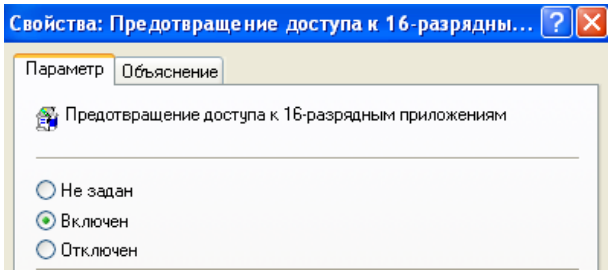


Рис. 5.43. Предотвращение доступа к 16-разрядным приложениям

- **Удаление команды «Свойства папки» из меню «Сервис»**

Откроем оснастку **«Удалить команду «Свойства папки» из меню «Сервис»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows»→ узел «Проводник» → узел«Удалить команду «Свойства папки» из меню «Сервис»***.**

Следует запрещать пользователю доступ к команде **«Свойства папки»**, поскольку, с ее использованием, можно настроить разрешение на отображение скрытых и системных файлов. Поскольку изменение системных файлов влечет ошибки в работе системы, их нельзя изменять обычным пользователям, не имеющим представления о том, как правильно настраивать систему. В целях безопасности уберем возможность обращения к свойствам папок (рис. 5.44):

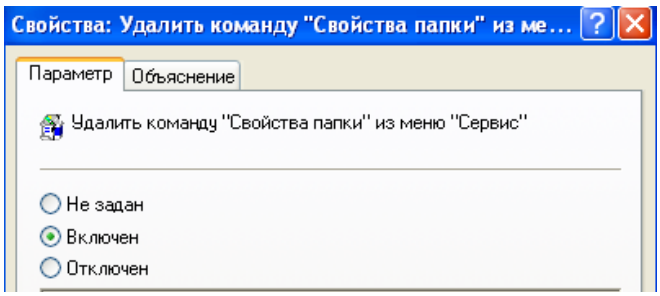


Рис. 5.44. Удаление команды «Свойства папки» из меню «Сервис»

- **Удаление вкладки «Безопасность»**

Откроем оснастку **«Удалить вкладку «Безопасность»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows»→узел «Проводник» → узел«Удалить вкладку «Безопасность».*

Политика безопасности для пользователя и АРМ настраивается системным администратором, в целях сохранения безопасности на должном уровне, нельзя допускать возможность изменения каких-то настроек из системы самим пользователем. Во избежание такой возможности уберем вкладку «Безопасность» (рис. 5.45):

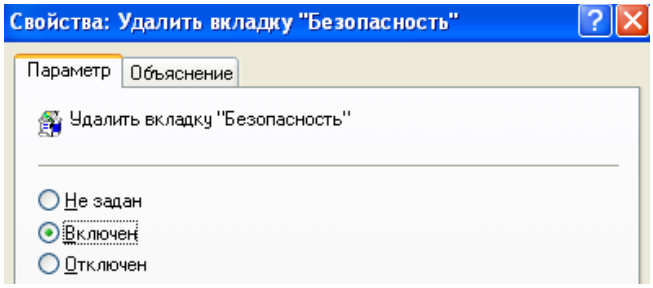


Рис. 5.45. Удаление вкладки «Безопасность»

- **Скрытие значка «Вся сеть» в папке «Сетевое окружение»**

Откроем оснастку **«Скрыть значок «Вся сеть» в папке «Сетевое окружение»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Проводник» → узел«Скрыть значок «Вся сеть» в папке «Сетевое окружение».*

Знание топологии сети для обычного пользователя не должно представлять интереса, однако в случае, если к данному АРМ получит доступ злоумышленник, это облегчит ему понимание того, как следует действовать дальше. Поэтому в целях безопасности следует убрать возможность просмотра полной топологии сети (рис. 5.46):

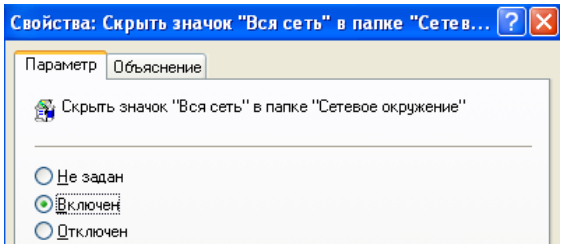


Рис. 5.46. Скрытие значка «Вся сеть»

- **Запретить создание новых заданий**

Откроем оснастку **«Запретить создание новых заданий»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows»→ узел «Планировщик заданий» → узел«Запретить создание новых заданий».*

Все задания, которые запланированы в системе, задаются системным администратором. Следует запретить возможность создания новых заданий самим пользователем (рис.5.47):

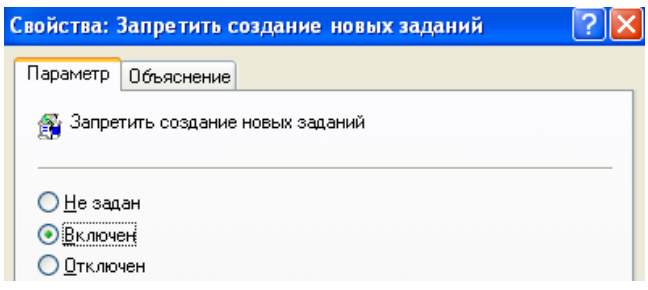


Рис. 5.47. Запрет создания новых заданий

- **Запретить удаление заданий**

Откроем оснастку **«Запретить удаление заданий»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows» → узел «Планировщик заданий» → узел«Запретить удаление заданий».*

Все задания, которые запланированы в системе, задаются системным администратором. Следует запретить возможность удаления уже установленных заданий самим пользователем (рис.5.48):

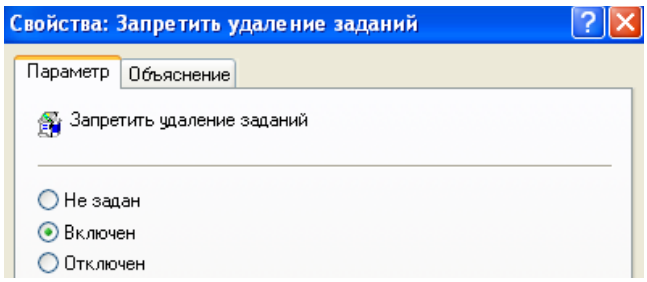


Рис. 5.48. Запрет удаления заданий

- **Запрет использования съемных носителей при установке**

Откроем оснастку **«Запретить использование съемных носителей при установке»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Компоненты Windows»→ узел «Установщик Windows» → узел«Запретить использование съемных носителей при установке».*

Политика безопасности предприятия подразумевает, что пользователям нельзя использовать личные съемные носители. В целях повышения безопасности следует запретить использование любых съемных носителей для установки каких бы то ни было приложений (рис.5.49):

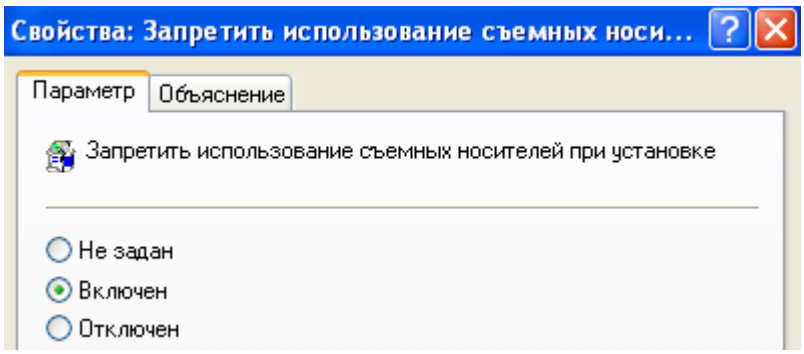


Рис. 5.49. Запрет использования съемных носителей при установке

- **Удаление «Сетевых подключений» из меню «Пуск»**

Откроем оснастку **«Удалить «Сетевые подключения из меню «Пуск»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Панель задач и меню «Пуск» → узел«Удалить «Сетевые подключения из меню «Пуск».*

Ранее в политике «Конфигурация Windows» был настроен запрет возможности выхода в сеть для пользователей: был выбран неправильный прокси-сервер, чтобы запросы пользователя оставались без ответа и, соответственно, доступ в интернет не работал. Теперь для увеличения безопасности следует убрать вкладку «Сетевые подключения» из меню «Пуск», чтобы пользователь не имел возможности выбрать другой прокси-сервер и восстановить подключение к интернету (рис.5.50):

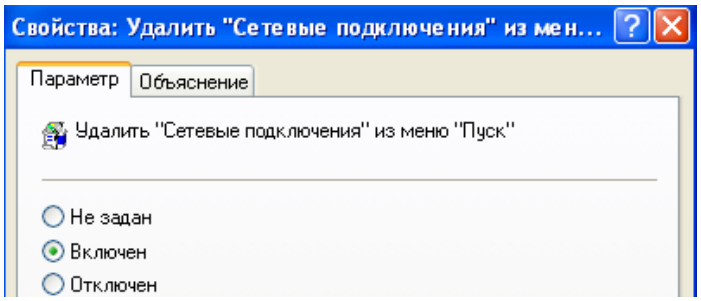


Рис. 5.50. Удаление «Сетевых подключений» из меню «Пуск»

- **Действия при отключении от сервера**

Откроем оснастку **«Действия при отключении от сервера»**, перейдя по адресу: *WIN+R → gpedit.msc → оснастка «Групповые политики» → узел «Конфигурация пользователя» → узел «Административные шаблоны» → узел «Сеть» → узел«Автономные файлы» → узел«Действия при отключении от сервера».*

Поскольку синхронизация с сервером важна для АРМ и, соответственно, для пользователя, работающего за ней, следует предусмотреть порядок работы в случае, если сервер окажется недоступен. Для этого включим параметр **«Действия при отключении сервера»** и укажем реакцию системы, когда сервер становится недоступен: система будет работать автономно, т.е. файлы сервера будут доступны локальному компьютеру. Эта настройка позволит избежать простоев и финансовых убытков, связанных с ними.

«Административные шаблоны» оснастки **«Конфигурация Windows»** успешно настроена (рис. 5.51).

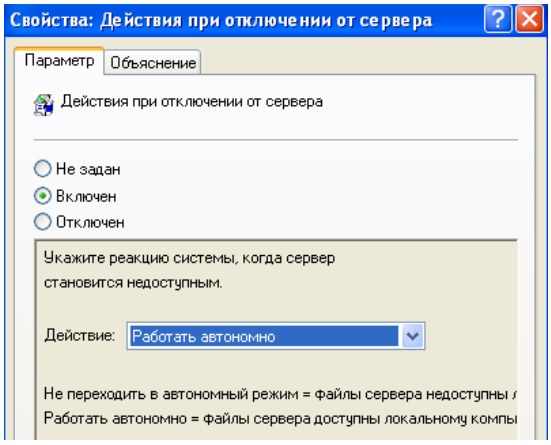


Рис. 5.51. Действия при отключении от сервера

«Административные шаблоны» оснастки **«Конфигурация пользователя»** успешно настроена.

Промежуточный вывод: в процессе выполнения данного этапа задания были настроены «Административные шаблоны» с учетом места расположения АРМ. Приведены обоснования настроек параметров для каждого пункта политики безопасности. Также дополнительно были настроены параметры безопасности ОС: с помощью данной оснастки были исключены команды и вкладки, использованием которых пользователь смог бынарушить работоспособность АРМ. Например, была удалена возможность получить доступ к «Свойствам папок», через которые можно открыть системные файлы, а также возможность просмотра «Соединения», что не позволит пользователям попытаться сменить прокси-сервер и получить доступ в сеть. Также был настроен порядок работы системы в случае, если сервер будет недоступен, чтобы избежать простоя и финансовых убытков, связанных с ними.

На этом настройка узла **«Конфигурация пользователя»** закончена.

Вывод по пункту: в данной части лабораторной работе были настроены политики, относящиеся к узлу **«Конфигурация пользователя»**, предназначенному для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему.

Дочерний узел «Конфигурация программ» позволяет указать определенную процедуру установки программного обеспечения.

Дочерний узел «Конфигурация Windows» в основном предназначен для обеспечения безопасности компьютера и учетной записи, для которой применяются данные политики.

Дочерний узел «Административные шаблоны» является крупнейшим из всех возможных расширений групповой политики и включает тысячи параметров для приложений и компонентов операционной системы Windows.

В частности, в процессе выполнения данного задания были настроены:

- Конфигурация Windows, включая сценарии для входа и выхода пользователя из системы, направленные на резервирование данных
- Произведена настройка политики «Настройки InternetExplorer», заключающиеся в основном в запрете пользователю доступа в интернет в целях безопасности данных, хранящихся на АРМ
- Административные шаблоны, включающие в себя компоненты для безопасной работы пользователя на АРМ

Каждый параметр политик и журналов был аргументирован в соответствии с выбранной ролью АРМ, указанной в начале каждого пункта.

Для каждого этапа настройки политик представлен свой промежуточный вывод по этапу, суммирующий проделанную в ходе выполнения каждой задачи работу.

Выводы по лабораторной работе: в данной лабораторной работе были изучены групповые политики безопасности АРМ. В частности, были настроены:

- Политика «Конфигурация компьютера», предназначенная для настройки параметров компьютера, применяемых невзирая на то, под какой учетной записью пользователь вошел в систему
- Политика «Конфигурация пользователя», предназначенная для настроек параметров пользователей. Параметры, которые находятся в этом узле, применяются при входе конкретного пользователя в систему
- Для каждой из политик, упомянутых выше, были настроены дочерние узлы «Конфигурация Windows», включая «Сценарии» и «Параметры безопасности», и «Административные шаблоны»

Каждый параметр политик и настроек их дочерних узлов был аргументирован в соответствии с выбранной ролью АРМ, указанной в начале каждого пункта.

Для каждого пункта задания представлен свой вывод по пункту, суммирующий проделанную в ходе выполнения каждой задачи работу.

6. Содержание отчета

6.1. Сформулировать цель выполнения работы

6.2. Обосновать критерии выбора опций и политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя» согласно заданию.

6.3. Привести и обосновать настройки каждого параметра групповых политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя».

6.4. Указать последовательность команд для выхода в диалоговые окна настройки параметров для каждой политики безопасности дочерних узлов.

6.5. Привести скриншоты до и после настройки параметров групповых политик безопасности дочерних узлов.
6.6. Сформулировать выводы значимости настроек каждой групповой политики безопасности для защиты АРМ от НСД.

7. Контрольные вопросы

7.1. Какие основные угрозы нарушения базовых услуг безопасности «конфиденциальность», «целостность» и «доступность» ресурсов АРМ?
7.2. Какие требования по защите АРМ от НСД «закрытого» и «открытого» контура ИС?
7.3. Как производятся настройки опций и политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя»?
7.4. Что лежит в основе критериев выбора политик безопасности?
7.5. Укажите мотивации настройки каждого параметра групповых политик безопасности дочерних узлов «Конфигурация Windows» и «Административные шаблоны» для узлов «Конфигурация компьютера» и «Конфигурация пользователя».

ЛАБОРАТОРНАЯ РАБОТА № 3 «АДМИНИСТРИРОВАНИЕ И НАСТРОЙКА ПОЛИТИКИ БЕЗОПАСНОСТИ СЕРВЕРА РЕЛЯЦИОННОЙ БАЗЫ ДАННЫХ»

1. Цель работы

– изучить команды MySQL и систему привилегий (privilegesystem). Научиться устанавливать и администрировать SQL−сервер на примере сервера MySQL, а также настраивать его параметры безопасности.

Используемое программное обеспечение: ОС версии не ниже Windows7, ПО сервера MySQL.

2. Задание к лабораторной работе

2.1. Установить макет варианта лабораторной работы на диск С (VirtualBox).
2.2. Установить сервер MySQL (на любую операционную систему).
2.3. Создать новую базу данных (с произвольным именем).
2.4. Создать пользователя MySQL с полным доступом к созданной на шаге 3 базе только с локального хоста. Осуществить соединение с сервером от имени созданного пользователя. Дальнейшая работа (шаги 4−7) производится от имени данного пользователя.

2.5. Создать (как пример) таблицу телефонного справочника (с произвольным именем) в созданной на шаге 6 базы, имеющей следующие колонки:

- UserName – типданных Text
- UserAddress – типданных Text
- UserPhone – тип данных Text

2.6. Заполнить таблицу произвольными значениями (5-6 записей).

2.7. Настроить параметры безопасности −права пользователя по доступу к управлению сервером и к базе данных, отдельным таблицам и полям таблиц, а также встроенным функциям и хранимым процедурам.

2.8. Сделать выборку из таблицы значения адреса и телефона для указанного UserName (любое из имен, введенных на шаге 5).

2.9. Сделать выборку из таблицы с сортировкой по полю UserName в алфавитном порядке.

2.10. Соединиться с сервером от имени администратора (root) и удалить созданных пользователя, таблицу и базу данных.

2.11. Указать последовательность команд SQL, используемую при выполнении задания, с комментариями по каждой команде, а также ответы сервера

2.12. Объяснить критерии выбора настроек и обосновать настройку параметров доступа из клиента базы данных (программы mysql.exe) по доступу к управлению сервером и к отдельным таблицам и полям таблиц, а также встроенным функциям и хранимым процедурам. Объяснить значимость настроенной политики безопасности для защиты базы данных от НСД.

3. Краткие теоретические сведения

3.1. Реляционные базы данных. Общие сведения

Задача длительного хранения и обработки информации появилась практически сразу с появлением первых компьютеров. Для решения этой задачи в конце 60-х годов были разработаны специализированные программы, получившие название систем управления базами данных (СУБД). СУБД проделали длительный путь эволюции от системы управления файлами, через иерархические и сетевые базы данных. В конце 80-х годов доминирующей стала система управления реляционными базами данных (СУРБД). С этого времени такие СУБД стали стандартом де-факто, и для того, чтобы унифицировать работу с ними, был разработан структурированный язык запросов (SQL), который представляет собой язык управления именно реляционными базами данных.

Существуют следующие разновидности баз данных:

- иерархические;
- реляционные;
- объектно-ориентированные;
- гибридные.

Иерархическая база данных основана на древовидной структуре хранения информации. В этом смысле иерархические базы данных очень напоминают файловую систему компьютера.

В **реляционных** базах данных данные собраны в таблицы, которые в свою очередь состоят из столбцов и строк, на пересечении которых расположены ячейки. Запросы к таким базам данных возвращает таблицу, которая повторно может участвовать в следующем запросе. Данные в одних таблицах, как правило, связаны с данными других таблиц, откуда и произошло название «реляционные».

В **объектно-ориентированных** базах данных данные хранятся в виде объектов. С объектно-ориентированными базами данных удобно работать, применяя объектно-ориентированное программирование. Однако, на сегодняшний день такие базы данных еще не достигли популярности реляционных, поскольку пока значительно уступают им в производительности.

Гибридные СУБД совмещают в себе возможности реляционных и объектно-ориентированных баз данных.Эти модели характеризуются простотой структуры данных, удобным для пользователя табличным представлением и возможностью использования формального аппарата алгебры отношений и реляционного исчисления для обработки данных.

Понятие реляционный (англ. *relation* — отношение) связано с разработками известного английского специалиста в области систем баз данных Эдгара Кодда (EdgarCodd). Модель реляционной базы данных представляет данные в виде таблиц, разбитых на строки и столбцы, на пересечении которых находятся данные. Кратко особенности реляционной базы данных можно описать следующим образом:

- Данные хранятся в таблицах, состоящих из столбцов и строк;
- На пересечении каждого столбца и строчки стоит в точности одно значение;
- У каждого столбца есть своё имя, которое служит его названием, и все значения в одном столбце имеют один тип. Например, в столбце id_forum все значения имеют целочисленный тип, а в строке name - текстовый;
- Столбцы располагаются в определённом порядке, который определяется при создании таблицы, в отличие от строк, которые располагаются в произвольном порядке. В таблице может не быть не одной строчки, но обязательно должен быть хотя бы один столбец;
- Запросы к базе данных возвращают результат в виде таблиц, которые тоже могут выступать как объект запросов.

Для работы с базами данных используется язык SQL(StructuredQueryLanguage — язык структурированных запросов). Стандарт SQL определен ANSI (AmericanNationalStandartInstitute). SQL предназначен для манипуляции данными, которые хранятся в Системах управления реляционными базами данных (RDBMS). SQL имеет команды, с помощью которых данные можно извлекать, сортировать, обновлять, удалять и добавлять. Стандарты языка SQL определяет ANSI

(AmericanNationalStandardsInstitute). Однако SQL не является изобретением ANSI, он – продукт исследования фирмы IBM, проводимого в начале 70-х годов 20 века. Другие организации и учебные заведения также внесли вклад в создание этого языка, например, компания Oracle или Калифорнийский университет Беркли. В настоящее время действует стандарт, принятый в 2003 году (SQL-3).

SQL можно использовать с такими базами RDBMS как MySQL, mSQL, PostgreSQL, Oracle, Microsoft SQL Server, Access, Sybase, Ingres. Эти системы RDBMS поддерживают все важные и общепринятые операторы SQL, однако каждая из них имеет множество своих собственных патентованных операторов и расширений.

SQL является общим языком запросов для нескольких баз данных различных типов.

*3.2. **База данных MySQL. Общие сведения***

MySQL, которая является RDBMS с открытым исходным кодом, доступна для загрузки на сайте MySQL.com. Разработчиком MySQLявляется компания MySQL AB. В настоящее время компания куплена корпорацией Oracle, которой и принадлежит теперь продукт. Свое происхождение MySQL ведет от продукта mSQL, разработанного в конце 1970-х гг. компанией TcX и использовавшемуся для доступа к таблицам, для которых использовались собственные быстрые подпрограммы низкого уровня. Однако после тестирования был сделан вывод, что скорость и гибкость mSQL недостаточны. В результате для базы данных был разработан новый SQL-интерфейс. Новый продукт получил название MySQL.

Вот как характеризуют MySQL её разработчики.

- MySQL - это система управления базами данных.

  База данных представляет собой структурированную совокупность данных. Эти данные могут быть любыми - от простого списка предстоящих покупок до перечня экспонатов картинной галереи или огромного количества информации в корпоративной сети. Для записи, выборки и обработки данных, хранящихся в компьютерной базе данных, необходима система управления базой данных, каковой и является ПО MySQL. Поскольку компьютеры замечательно справляются с обработкой больших объемов данных, управление базами данных играет центральную роль в вычислениях. Реализовано такое управление может быть по-разному - как в виде отдельных утилит, так и в виде кода, входящего в состав других приложений.
- MySQL - это система управления реляционными базами данных.

  В реляционной базе данные хранятся в отдельных таблицах, благодаря чему достигается выигрыш в скорости и гибкости. Таблицы связываются между собой при помощи отношений, благодаря чему обеспечивается возможность объединять при выполнении запроса данные из нескольких таблиц. SQL как часть системы MySQL можно охарактеризовать как язык

структурированных запросов плюс наиболее распространенный стандартный язык, используемый для доступа к базам данных.

- Программное обеспечение MySQL - это ПО с открытым кодом.

ПО с открытым кодом означает, что применять и модифицировать его может любой желающий. Такое ПО можно получать по Internet и использовать бесплатно. При этом каждый пользователь может изучить исходный код и изменить его в соответствии со своими потребностями. Укажем важные характеристики программного обеспечения MySQL:

- Внутренние характеристики и переносимость
  - Написан на C и C++. Протестирован на множестве различных компиляторов.
  - Работает на различных аппаратных платформах и разных операционных системах.
  - Высокая производительность за счет максимально оптимизированного кода, эффективной системы распределения памяти и продуманной системы дисковых таблиц.
- Масштабируемость
  - Способность работать с очень большими базами данных (десятки и сотни миллионов записей).
  - Возможность кластеризации серверов и распределения обработки информации между серверами
- Технические возможности СУБД MySQL

ПО MySQL является системой клиент-сервер, которая содержит многопоточный SQL-сервер, обеспечивающий поддержку различных вычислительных машин баз данных, а также несколько различных клиентских программ и библиотек, средства администрирования и широкий спектр программных интерфейсов (API).

- Безопасность

Система безопасности основана на привилегиях и паролях с возможностью верификации с удаленного компьютера, за счет чего обеспечивается гибкость и безопасность. Пароли при передаче по сети при соединении с сервером шифруются. Клиенты могут соединяться с MySQL, используя сокеты TCP/IP, сокеты Unix или именованные каналы (namedpipes, под NT).

Клиентская программа MySQL представляет собой утилиту командной строки. Эта программа подключается к серверу по сети. Команды, выполняемые сервером, обычно связаны с чтением и записью данных на жестком диске. Клиентские программы могут работать не только в режиме командной строки. Есть и графические клиенты, например MySQL GUI, phpMyAdmin и др.

3.3. Краткий обзор команд MySQL

Создание базы данных выполняется с помощью команды **CREATE DATABASE**.

Синтаксискоманды:

CREATE DATABASE *database_name*

 database_name - Имя, которое будет присвоено создаваемой базе данных.

Для **удаления** базы данных используется команда **DROP DATABASE.**

Синтаксис:

DROP DATABASE *database_name*

где

 database_name - задает имя базы данных, которую необходимо удалить.

Создание таблицы производится командой **CREATE TABLE**.

CREATE TABLE table_name(column_name1 *type*, column_name2 *type*,...)

 table_name- имя новой таблицы;

 column_name - имена колонок (полей), которые будут присутствовать в создаваемой таблице.

 type - определяет тип данных создаваемой колонки.

Например, надо создать таблицу учетных записей и паролей с именем user_pass. Пусть таблица будет состоять из двух столбцов – UserName и UserPassword с типом данных text:

```
CREATE TABLE user_pass(UserName text, UserPassword text);
```

Удаление таблицы производится командой **DROP TABLE**

DROP TABLE *table_name*

table_name - имяудаляемойтаблицы.

Вставка записи осуществляется командой **INSERT INTO**

INSERT INTO *table_name*(field_name1, field_name2,...) values('content1', 'content2',...)

Данная команда добавляет в таблицу *table_name* запись, у которой поля, обозначеные как field_nameN, установлены в значение contentN.

Например, в таблицу учетных записей и паролей можно добавить запись следующим образом:

```
INSERT INTO user_pass(UserName, UserPassword)
        values('Operator', '1qAz_weR');
```

Поиск записей осуществляется командой **SELECT**

```
SELECT * FROM table_name WHERE (выражение) [order by field_name [desc][asc]]
```

Эта команда ищет все записи в таблице *table_name*, которые удовлетворяют выражению *выражение.*

Если записей несколько, то при указаном предложении orderby они будут отсортированы по тому полю, имя которого записывается правее этого ключевого слова (если задано слово desc, то упорядочивание происходит в обратном порядке). В предложении orderby могут также задаваться несколько полей. Особое значение имеет символ *. Он предписывает, что из отобранных записей следует извлечь все поля, когда будет выполнена

команда получения выборки. С другой стороны, вместо звездочки можно через запятую непосредственно перечислить имена полей, которые требуют извлечения.

Например, выбрать все записи из таблицы можно следующим образом:

```
SELECT * FROMuser_pass;
```

Выбрать все записи с сортировкой по имени в обратном алфавитном порядке:

```
SELECT * FROM user_pass ORDER BY UserNamedesc;
```

Выбрать пароль для пользователя Admin:

```
SELECT UserPassword FROM user_pass WHERE UserName=’Admin’;
```

4. Последовательность выполнения работы

4.1. ***Установить макет варианта лабораторной работы на диск C (VirtualBox).***

4.2. ***Установить MySQL на платформу ОС Windows7 и выше***

Дистрибутив можно скачать с www.mysql.com. On-linedокументация (на английском языке) расположена по адресу http://dev.mysql.com/doc/

Для установки необходимо иметь административные права. Перед установкой необходимо установить MicrosoftNetFramework 4.0, использующийся в программах администрирования в среде MicrosoftWindows. Для других операционных систем используются другие методы администрирования.

Непосредственно процесс установки производится аналогично другим программам в Windows, поэтому здесь не рассматривается. При выборе типа устанавливаемого сервера рекомендуется выбрать пользовательскую установку (допускается выбрать полную, но будут установлены неиспользуемые компоненты и потребуется дополнительно установить библиотеку Visual C++ 2010 Runtime, не входящую в дистрибутив). Обязательно должны быть установлены (рис. 4.1.):

- Вгруппе «MySQL Server 5.6.11» - MySQL Server, Client Programs, Server Data Files.
- Вгруппе Applications – MySQL Notifier.
- Группу MySQLConnectors – не устанавливать
- Группу Documentation – рекомендуется установить полностью.

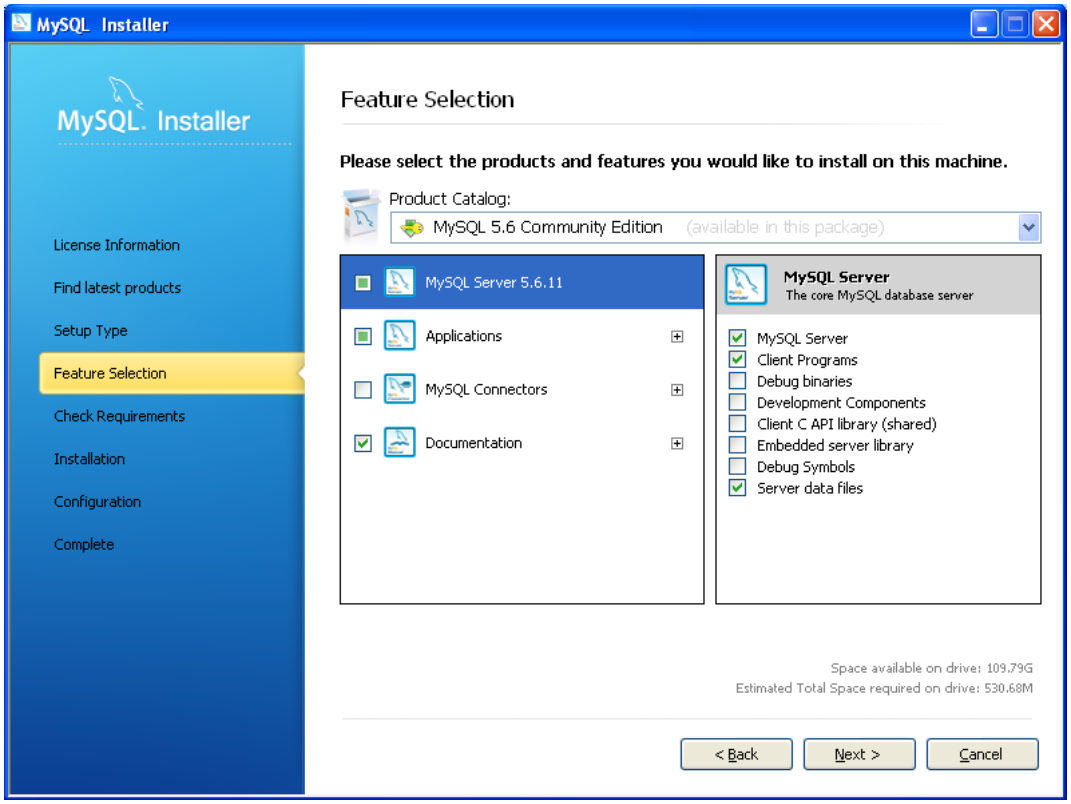


Рис. 4.1. Рекомендуемые установки ПО

После окончания установки запускается Мастер настроек MySQL (он также доступен пользователю и после инсталляции).

4.2.1. *Окно настройки серверной части. Рекомендуется выбрать конфигурацию «DevelopmentMachine» (рис.4.2).*

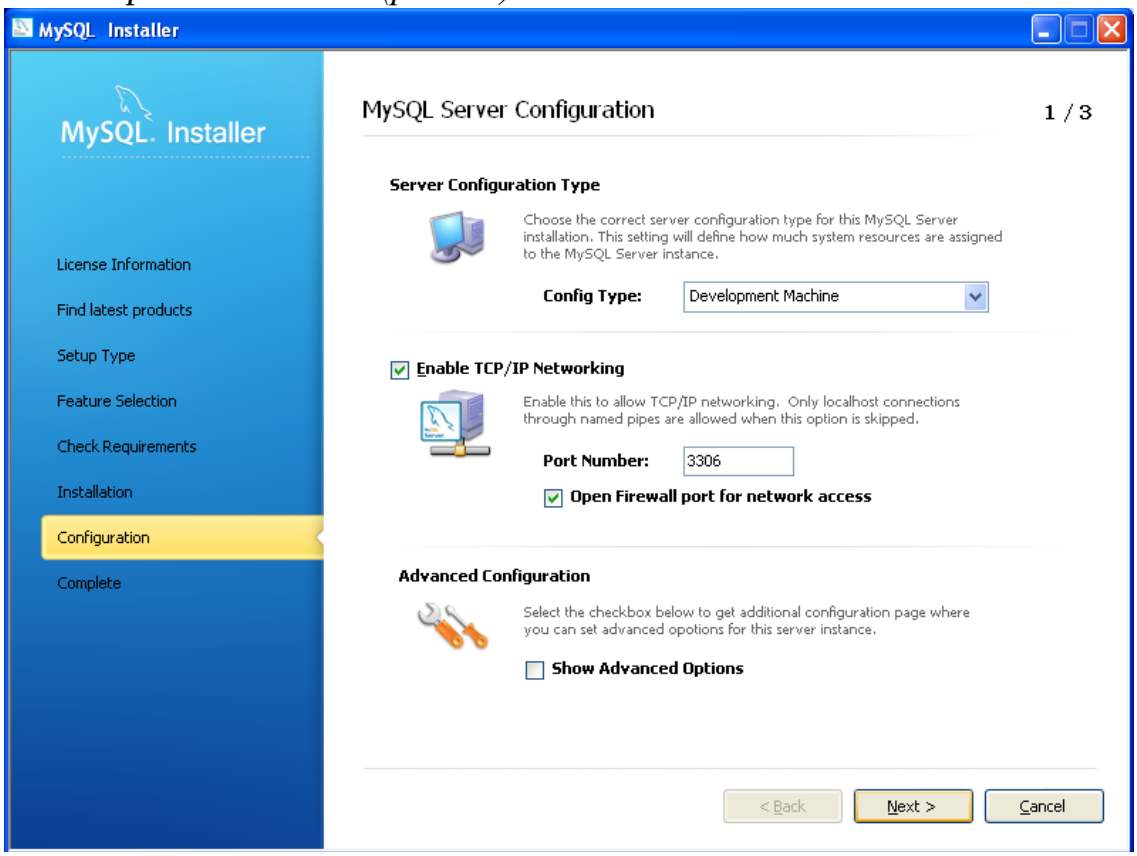


Рис.4.2. Окно настройки серверной части

4.2.2. Настроить пароль(учетная запись – root) главного администратора сервера (рис.4.3).

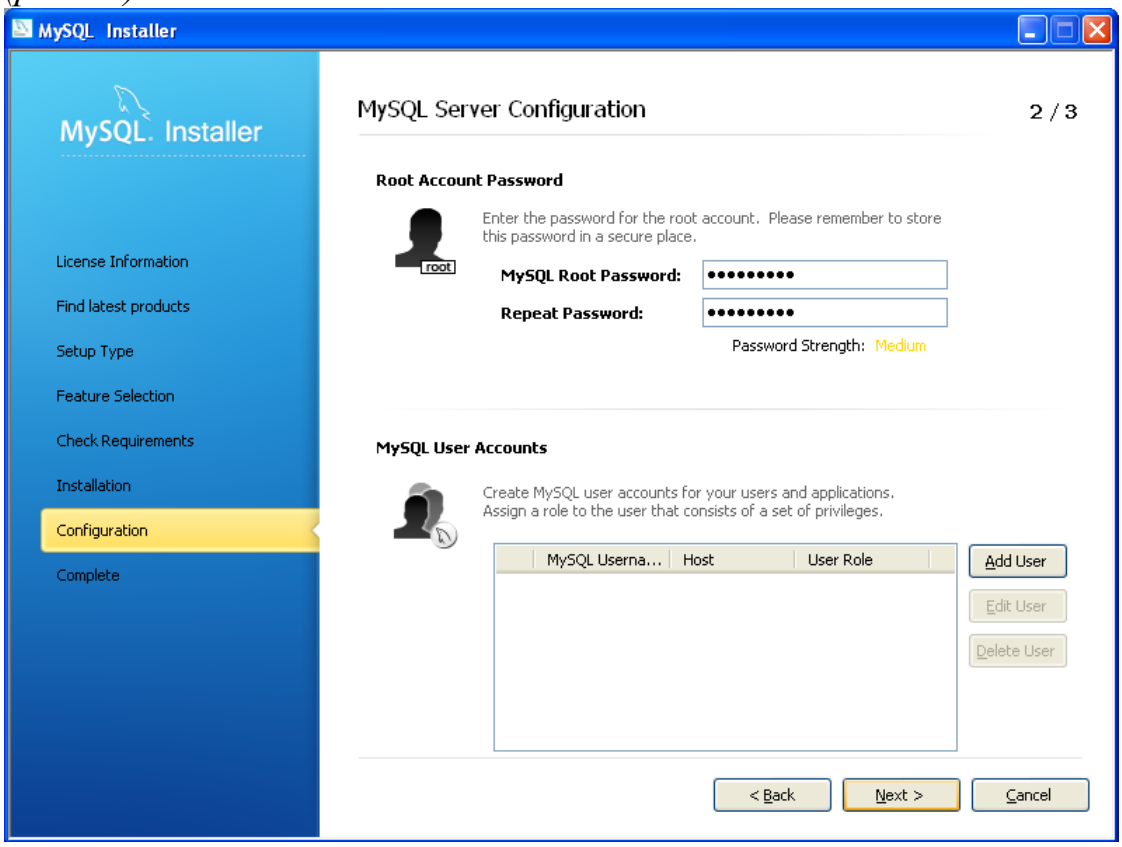


Рис.4.3. Настройка пароля главного администратора сервера (учетная запись – root)

4.2.3. При необходимости добавить дополнительных пользователей, установить им необходимый уровень доступа.

4.2.4. Окно настройка запуска сервиса оставить без изменений (рис.4.4).

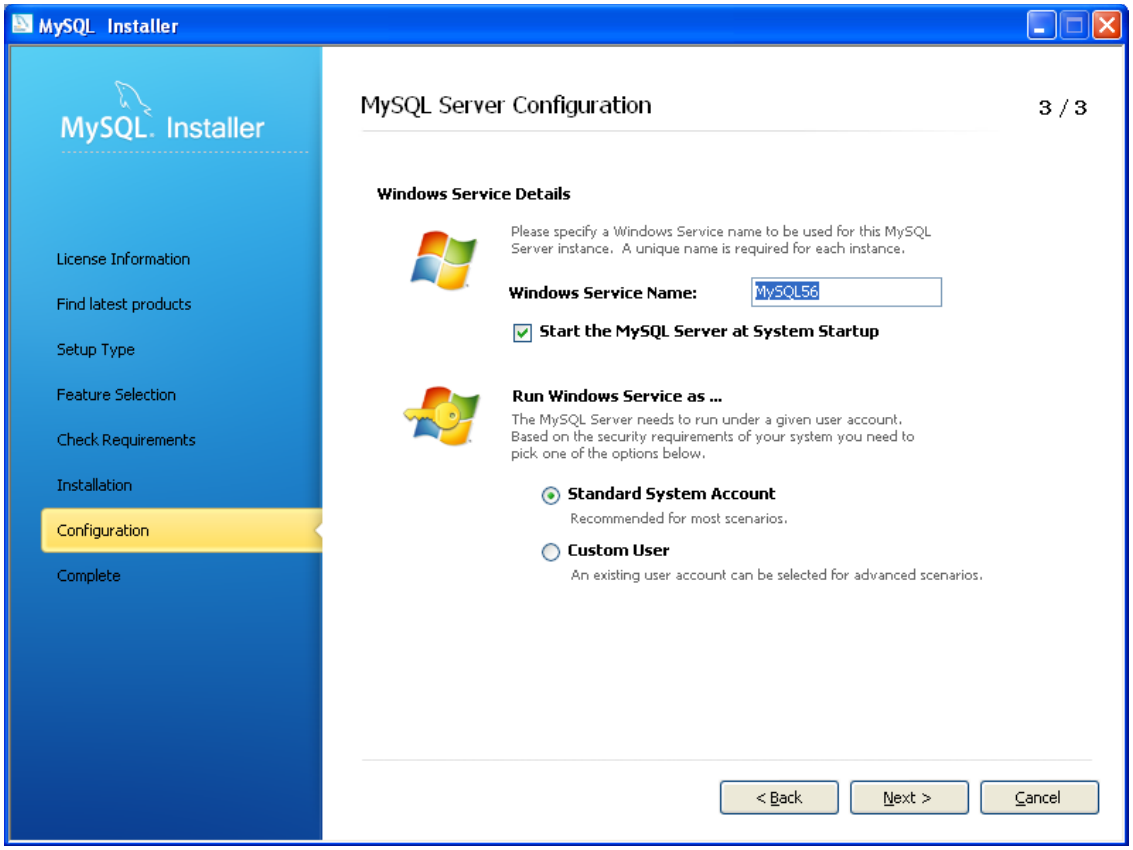


Рис.4.4. Окно настройка запуска сервиса

4.2.5. *На следующем этапе производится автоматическая настройка сервера в соответствии с заданной конфигурацией и его запуск.*

Для управления сервером используется утилита «MySQLNotifier» (вызывается из меню программ). Утилита выводит иконку в панели задач, являющуюся индикатором состояния сервера базы данных, а также позволяющую управлять сервером (запуск и останов сервера).

4.3. *Создать базу данныхMySQL*

4.4. *Настроить параметры безопасности*

Основой системы безопасности является система привилегий (privilegesystem), позволяющая очень гибко управлять правами доступа как к управлению сервером, так и к отдельным базам, таблицам и полям таблиц, а также встроенным функциям и хранимым процедурам. Для изучения всей системы привилегий рекомендуется обратиться к документации на программу, здесь же рассмотрим основные моменты.

Настройку параметров доступа можно производить из клиента базы данных – программы mysql.exe (находится в каталоге установки продукта в подкаталоге *bin*). При запуске программе можно указать много параметров, но для изучения достаточно использовать синтаксис:

mysql.exe –u<имя пользователя> -p<база данных>,

-u – флаг, за которым через пробел указывается имя пользователя

-p – флаг, указывающий на необходимость запроса пароля

<*база данных*> - имя базы, с таблицами которой будет проводиться работа. Этот параметр не является обязательным, т.к. из клиента в любой момент можно переключиться на работу с другой базой с использованием команды «use<база данных>».

Внимание! Все команды, вводимые в клиенте, обязательно должны заканчиваться точкой с запятой.

Все параметры безопасности MySQL хранятся в виде таблиц системной базы данных «mysql», поэтому первый запуск клиента рекомендуется осуществить командой

mysql.exe –uroot –pmysql (пароль был установлен в процессе инсталляции)

Создадим нового пользователя с заданным паролем:

CREATE USER 'имяпользователя'@'localhost' IDENTIFIED BY 'пароль';

В данном примере localhost означает, что пользователю будет доступен только локальный вход.

Предоставим пользователю полные права на все таблицы созданной при инсталляции программы базу данных test:

GRANT ALL PRIVILEGES ON test.* TO 'имя пользователя'@'localhost';

В данном примере *test.** означает все таблицы базы test. При необходимости можно предоставить права на отдельную таблицу (например, на таблицу table), указав *test.table*.

Для проверки прав доступа необходимо выполнить команду:

SHOW GRANTS FOR 'имяпользователя'@'localhost';

Удаление прав пользователя производится, например, следующим образом:

REVOKE ALL PRIVILEGES ON test.* FROM 'имя пользователя'@'localhost';

Выход из программы клиента осуществляется командой QUIT (можно без точки с запятой на конце).

Если теперь попробовать соединиться от имени созданного пользователя с базой mysql, то соединение будет отвергнуто сервером. Соединение же с базой test будет успешно установлено.

5. Методические рекомендации по выполнению работ

5.1. Установка MySQL на платформу ОС Windows

Установка MySQL возможна на ОС Windows 2000 и выше. Дистрибутив можно скачать с www.mysql.com. Онлайн-документация (на английском языке) расположена по адресу http://dev.mysql.com/doc/

Для установки необходимо иметь административные права (рис.5.1):

Рис. 5.1. Подтверждение прав администратора на локальной учетной записи

Очевидно, что на используемом АРМ (с установленной операционной системой Windows 8.1), используется учетная запись с правами администратора.

Непосредственно процесс установки производится аналогично другим программам в Windows, поэтому здесь не рассматривается. При выборе типа устанавливаемого сервера выбраны следующие параметры (рис.5.2):

- «MySQLServer» (в данной лабораторной работе будет использоваться «MySQLServer 8.0.18 - x64», стабильная версия для 64-х разрядных машин), в который входят MySQLServer, ClientPrograms, ServerDataFiles.
- «MySQLNotifier», утилита для управления сервером. Выводит иконку в панели задач, являющуюся индикатором состояния сервера базы данных, а также позволяющую управлять сервером (запуск и останов сервера).
- «MySQLDocumentation» для «MySQLServer 8.0.18 - x64», документация на английском языке для работы с сервером «MySQLServer 8.0.18 - x64», используемым в данной лабораторной работе.

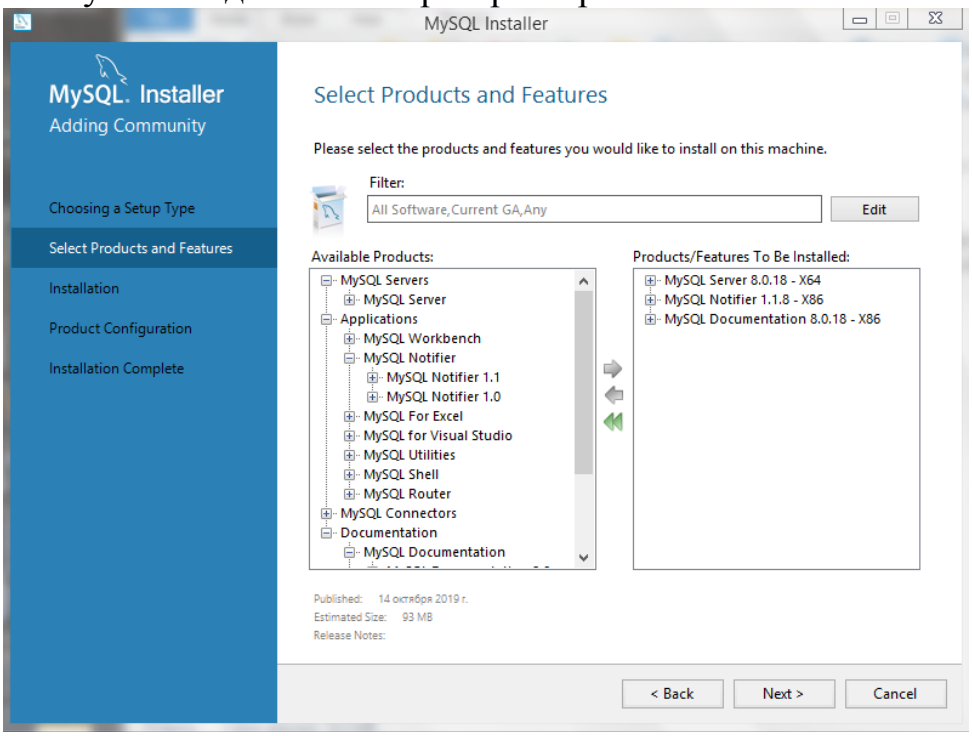


Рис. 5.2. Установка «MySQL»

Произвести настройку сервера «MySQLServer 8.0.18 - x64» с помощью «Мастера настроек MySQL), который запускается автоматически после установки вышеперечисленных компонентов. Настройка достаточно проста и интуитивно понятна, а поскольку цели лабораторной работы не предполагают реального использования всех ресурсов данного приложения, то большую часть параметров можно оставить «по умолчанию» – они автоматически подберутся под тип используемой операционной системы. Рассмотрим основные этапы настроек.

5.1.1. Окно настройки серверной части (рис.5.3)

Выберем конфигурацию «DevelopmentMachine» – этот тип установки предназначен для разработки и тестирования сайтов, в этом случае ресурсы компьютера будут подвергаться минимальной нагрузке. Поскольку цель лабораторной работы – ознакомиться с MySQL, посмотреть его основные возможности и функции, этой конфигурации будет достаточно. Однако, для продуктивной работы с «MySQLServer» и если планируется использовать полноценный веб-сервер с несколькими работающими сайтами, то необходимо выбирать тип конфигурации «ServerMachine», но это вариант для производительных компьютеров.

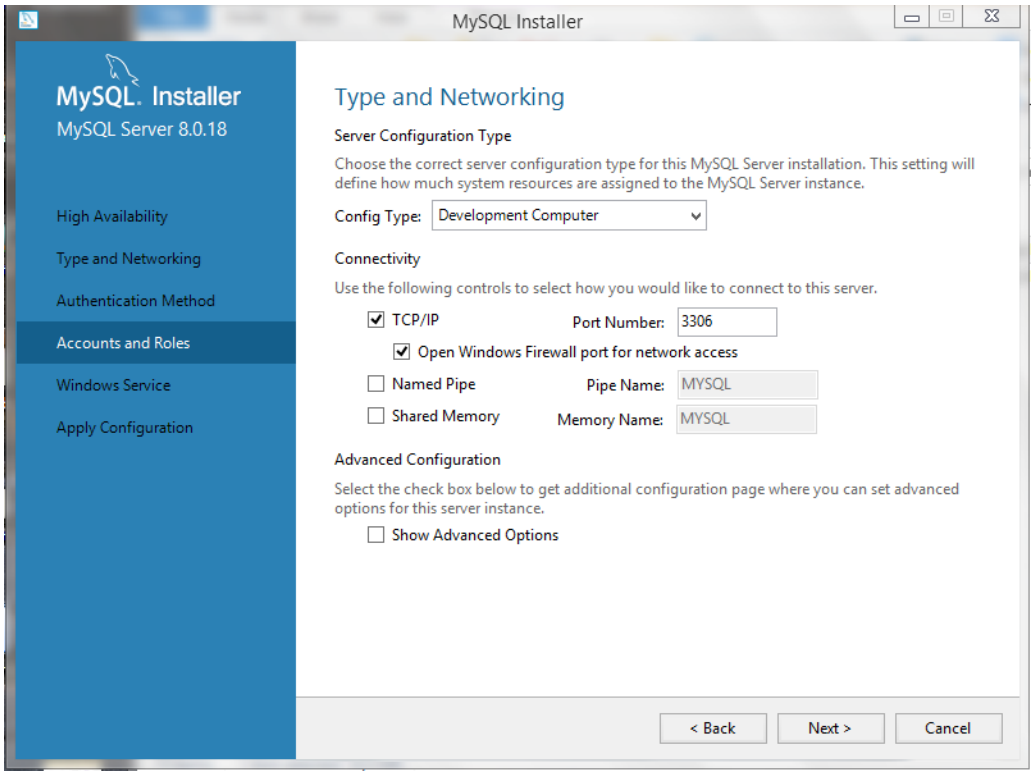


Рис. 5.3. Настройка серверной части

5.1.2. Настройка пароля главного администратора сервера (рис.5.4)

Данный параметр устанавливает пароль для пользователя «root». Оставлять это поле пустым не рекомендуется, поскольку в таком случае

любой может получить доступ к администрированию ваших баз данных, что негативно скажется на безопасности.

Предположим, что используемое АРМ установлено в «закрытом» контуре. Следовательно, нужно выбрать пароль соответствующей сложности для защиты доступа к базам данных для администратора (рис.5.4).Установим пароль P@ssword1234 – он соответствует принятым рекомендациям безопасности, содержит 12 символов и состоит из букв разного регистра, цифр и специальных символов (поскольку по рекомендациям безопасности оптимальное значение количества знаков для пароля серверов – от 10 до 12, наше АРМ не является сервером, но тем не менее должно защищаться лучше, чем обычное пользовательское место).

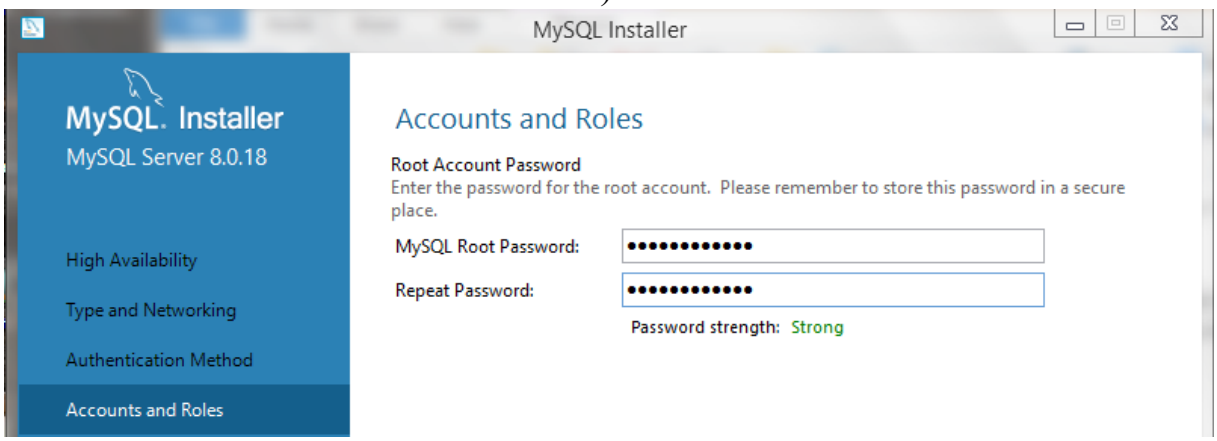


Рис. 5.4. Настройка пароля главного администратора

Также в этом пункте имеется возможность добавить дополнительных пользователей, установив им необходимый уровень доступа, но поскольку это входит в одно из заданий на выполнение лабораторной, то этот пункт будет рассмотрен далее.

5.1.3. *Окно автоматической настройки сервера в соответствии с заданной конфигурацией*

Применяет все раннее указанные настройки и автоматически применяет их на сервере. В результате выполнения показывает выполненные этапы и создает журнал применения изменений. На рис.5.5 можно видеть, что все настройки применены успешно, и что сервер MySQL готов к работе.

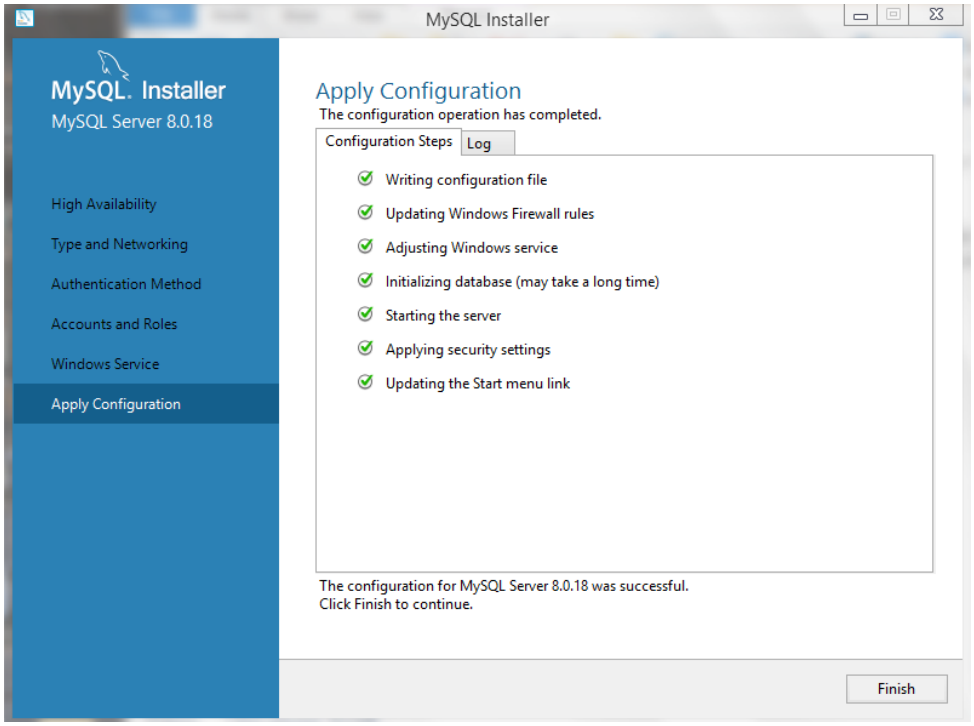


Рис. 5.5. Автоматическая настройка сервера в соответствии с заданной конфигурацией

Для дальнейшего управления сервером используется утилита «MySQLNotifier» (вызывается из меню программ). Утилита (рис.5.6) выводит иконку в панели задач, являющуюся индикатором состояния сервера базы данных, а также позволяющую управлять сервером (запуск и остановка сервера).

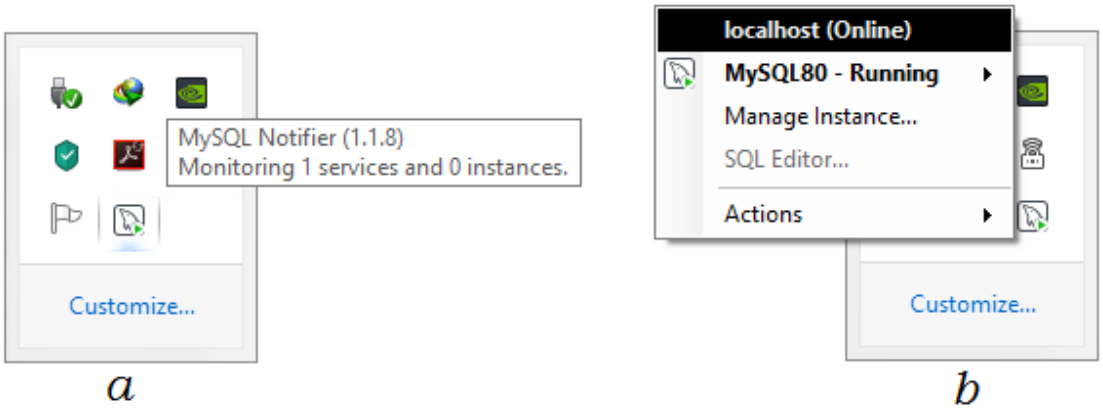


Рис.5. 6. Установленная утилита «MySQLNotifier» (a), взаимодействие с сервером с помощью средств утилиты (b)

На этом установка и предварительная настройка сервера «MySQLServer» завершена.

5.2. *Взаимодействие с сервером «MySQLServer» и настройка параметров безопасности*

5.2.1. *Краткий обзор команды SQL*

Перед тем, как приступить к выполнению данной части лабораторной работы, дадим краткий обзор команд для работы с SQL, которыми мы будет пользоваться в дальнейшем:

- Создание базы данных выполняется с помощью команды **CREATE DATABASE**.

  Синтаксискоманды:

  CREATE DATABASE *database_name*

  - *database_name* - Имя, которое будет присвоено создаваемой базе данных.
- Для **удаления** базы данных используется команда **DROP DATABASE**.

  Синтаксискоманды:

  DROP DATABASE *database_name*

  - *database_name* - задает имя базы данных, которую необходимо удалить.
- **Создание** таблицы производится командой **CREATE TABLE**.

  Синтаксискоманды:

  CREATE TABLE *table_name*(column_name1 *type*, column_name2 *type*,...)

  - table_name - имя новой таблицы;
  - column_name - имена колонок (полей), которые будут присутствовать в создаваемой таблице.
  - *type* - определяет тип данных создаваемой колонки.

  Например, надо создать таблицу учетных записей и паролей с именем user_pass. Пусть таблица будет состоять из двух столбцов – UserName и UserPassword с типом данных text:

```
CREATE TABLE user_pass(UserName text, UserPassword text);
```

- **Удаление** таблицы производится командой **DROP TABLE**

  Синтаксискоманды:

  DROP TABLE *table_name*

  - *table_name* - имя удаляемой таблицы.
- **Вставка записи** осуществляется командой **INSERT INTO**

  Синтаксискоманды:

  INSERT INTO *table_name*(field_name1, field_name2,...) values('content1', 'content2',...)

  Данная команда добавляет в таблицу *table_name* запись, у которой поля, обозначеные как field_nameN, установлены в значение contentN.

  Например, в таблицу учетных записей и паролей можно добавить запись следующим образом:

```
INSERT INTO user_pass(UserName, UserPassword)
  Values('Operator', '1qAz_weR');
```

- **Поиск записей** осуществляется командой **SELECT**

  Синтаксискоманды:

```
SELECT * FROM table_name WHERE (выражение) [order byfield_name [desc][asc]]
```

  Эта команда ищет все записи в таблице *table_name*, которые удовлетворяют выражению *выражение*.

Если записей несколько, то при указанном предложении *orderby* они будут отсортированы по тому полю, имя которого записывается правее этого ключевого слова (если задано слово *desc*, то упорядочивание происходит в обратном порядке). В предложении *orderby* могут также задаваться несколько полей. Особое значение имеет символ *. Он предписывает, что из отобранных записей следует извлечь все поля, когда будет выполнена команда получения выборки. С другой стороны, вместо звездочки можно через запятую непосредственно перечислить имена полей, которые требуют извлечения.

- Например, выбрать все записи из таблицы можно следующим образом:

```
SELECT * FROMuser_pass;
```

- Выбрать все записи с сортировкой по имени в обратном алфавитном порядке:

```
SELECT * FROM user_pass ORDER BY UserNamedesc;
```

- Выбрать пароль для пользователя Admin:

```
SELECT UserPassword FROM user_pass WHERE UserName=’Admin’;
```

Теперь можно приступать к выполнению заданий лабораторной работы.

5.2.2. Создание базы данных

На данный момент имеется настроенный сервер «MySQLServer» и утилита для взаимодействия с ним «MySQLNotifier». Для того, чтобы можно было использовать возможности сервера, такие как создание и назначение прав пользователям на таблицы и базы данных, требуется, собственно, сначала создать пользовательскую базу данных и таблицу в ней. Имеющиеся по умолчанию базы данных (рис.5.7) можно посмотреть с использованием команды

- showdatabases;

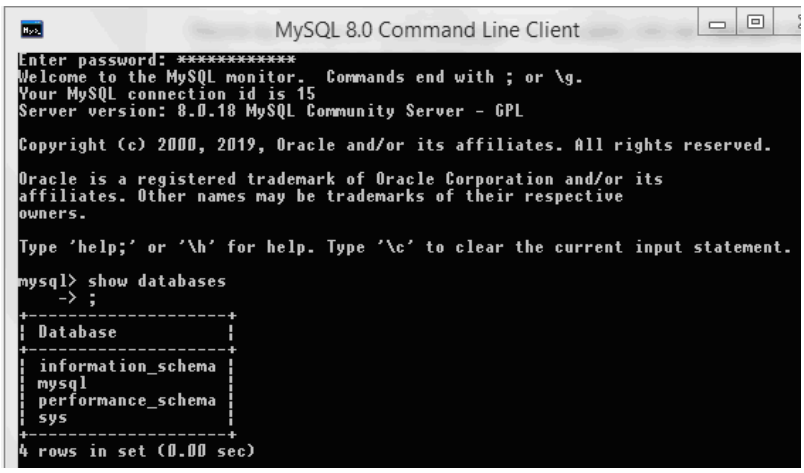


Рис.5. 7. Базы данных, созданные по умолчанию

Поскольку среди перечисленных баз данных имеются те, изменение данных в которых нежелательно (в частности, а базе данных mysql находится таблица user с перечнем всех пользователей, их паролей и способов подключения к базам данных), создадим собственную базу данных. Назовем ее laboratoryWork3 и создадим с помощью следующей команды:

- create database laboratoryWork3;

И используем ранее используемую команду просмотра существующих баз данных, чтобы проверить, создалась наша база данных или нет (рис.5.8):

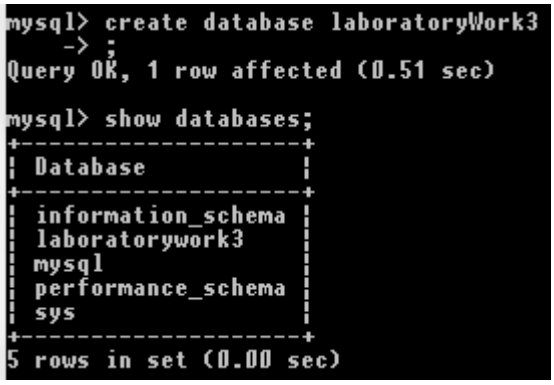


Рис. 5.8. Создание пользовательской базы данных и проверка результатов

Очевидно, база данных laboratoryWork3 успешно создана. Укажем серверу, что далее мы будем работать именно с ней, используя следующую команду (рис.5.9):

- use laboratoryWork3;

Рис. 5.9. Задание используемой в лабораторные базы данных

Очевидно, что пользовательская база данных создана успешно.

5.2.3. Создание нового пользователя и настройка его прав доступа

Приступим к выполнению самого важного задания, когда речь идет об администрировании баз данных: от того, какие права будут даны пользователю, что будет работать с базой данных, какие функции ему будут доступны, зависит целостность базы данных, связанных с ней таблиц и, соответственно, информации, что в них содержится. Неправильная настройка прав доступа и доступных возможностей может привести к искажению или даже потере информации.

После первоначальной настройки сервера MySQL, будет предоставлено имя пользователя и пароль, причем эти начальные учётные данные дают привилегии «root-доступа», то есть привилегированного пользователя. Пользователь с правами доступа root имеют полный доступ ко всем базам данных и таблицам внутри этих баз – но на предприятиях обычно требуется предоставить доступ к базе данных для работников, которым не требуется и не рекомендовано полное управление.

Для создания нового пользователя следует выполнить следующие шаги:

1) Создать пользователя MySQL и предоставить неограниченные права доступа
2) Назначить специальные права доступа для пользователя MySQL

5.2.3.1. Создание пользователя MySQL и предоставление ему неограниченных прав доступа

Создадим пользователя с именем LocalUser и установим ему пароль password. По заданию требуется создать локального пользователя – пользователя, который будет существовать на текущей АРМ. Это логично с точки зрения безопасности: нет необходимости создавать глобального пользователя, который будет иметь возможность войти в свою учетную запись с любого АРМ – в этом случае требовалось бы устанавливать какие-то дополнительные политики безопасности на каждом АРМ, с которого можно осуществить работу. В нашем случае достаточно будет настроить, скажем, локальные политики безопасности (см. лаб. раб. 1) и ограничить пользователю доступ в интернет только одним IP адресом – тем, на котором работает сервер MySQL.

Для этого выполним следующую команду (рис.5.10):

- create user ‘LocalUser’@’localhost’ identified by ‘password’;

```
mysql> create user 'LocalUser'@'localhost' identified by 'password';
Query OK, 0 rows affected (0.09 sec)
```

Рис. 5.10. Создание локального пользователя LocalUser с паролем password

Теперь необходимо назначить для созданного пользователя права доступа, сначала следует предоставить ему все права, а потом настроить в соответствии с политикой безопасности предприятия и регламентом работы с базами данных. Чтобы назначить вновь созданному пользователю неограниченные права доступа к нашей пользовательской базе данных laboratoryWork3, выполним следующую команду (рис.5.11):

- grant all privileges on laboratoryWork3.* to 'LocalUser'@'localhost';

```
mysql> grant all privileges on laboratoryWork3.* to 'LocalUser'@'localhost';
Query OK, 0 rows affected (0.68 sec)
```

Рис. 5.11. Установка прав доступа пользователю LocalUser

Теперь проверим, применились ли права, просмотрев их для пользователя с помощью команды (рис.5.12):

- show grants for ‘LocalUser’@’localhost’;

```
mysql> show grants for 'LocalUser'@'localhost';
+-----------------------------------------------------------------------+
| Grants for LocalUser@localhost                                        |
+-----------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `LocalUser`@`localhost`                         |
| GRANT ALL PRIVILEGES ON `laboratorywork3`.* TO `LocalUser`@`localhost` |
+-----------------------------------------------------------------------+
2 rows in set (0.00 sec)
```

Рис. 5.12. Просмотр прав пользователя LocalUser

Очевидно, что создание нового пользователя и применение к нему первоначальных прав доступа успешно осуществлено.

Организация доступа не привилегированного пользователя к серверу. Попробуем подключиться к серверу MySQL с помощью утилиты «MySQLWorkbench». Дополнительно установим ее с помощью той же программы, которой мы устанавливали «MySQLServer» (рис.5.13):

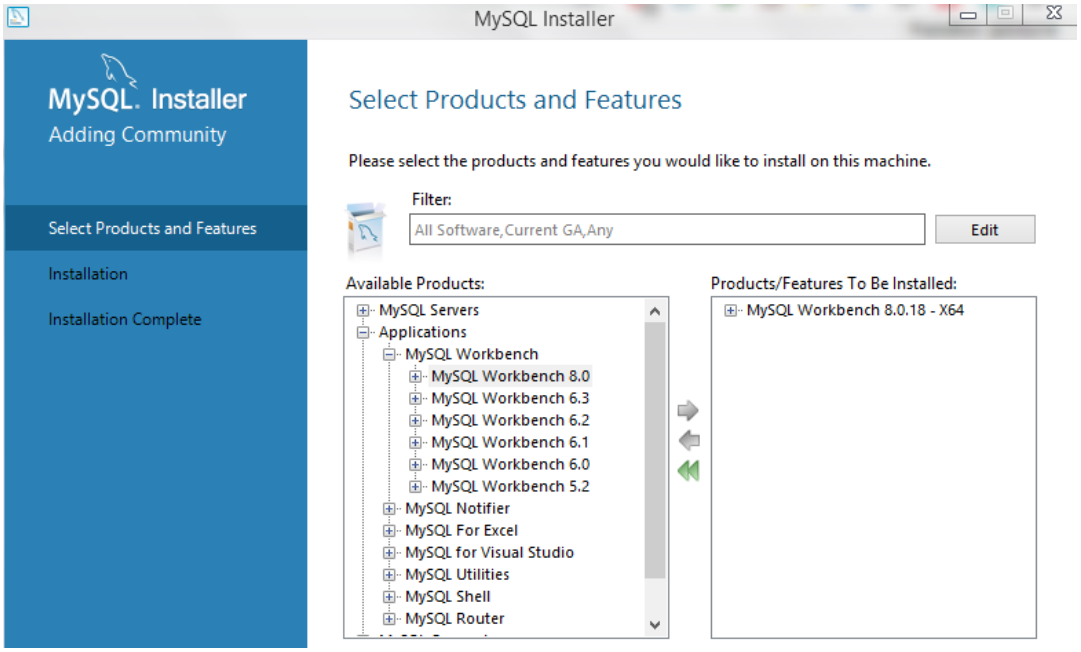


Рис. 5.13. Установка «MySQLWorkbench»

Чтобы запустить командную строку под новым пользователем необходимо зайти в интерфейс программы «MySQLWorkbench» и создать новое подключение, вызвав *ManageServerConnections*, для которого настроить следующие параметры, а остальные оставить по умолчанию:

- Connection Name: LocalUser
- Password: password

После настройки *ManageServerConnections* должен выглядеть следующим образом (рис.5.14):

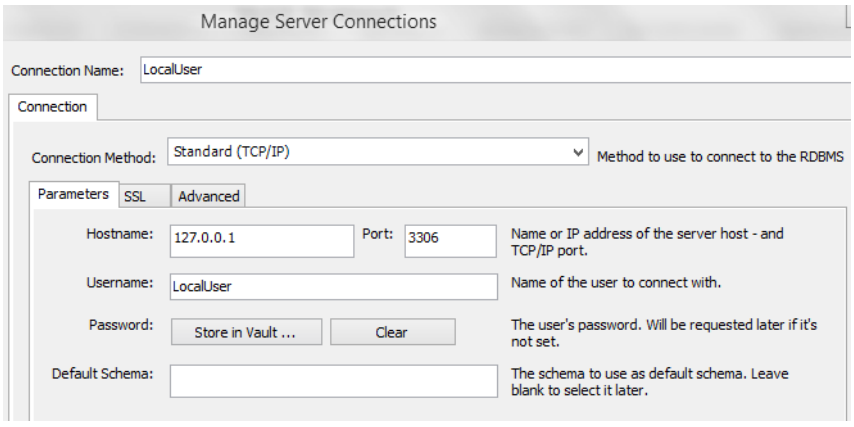
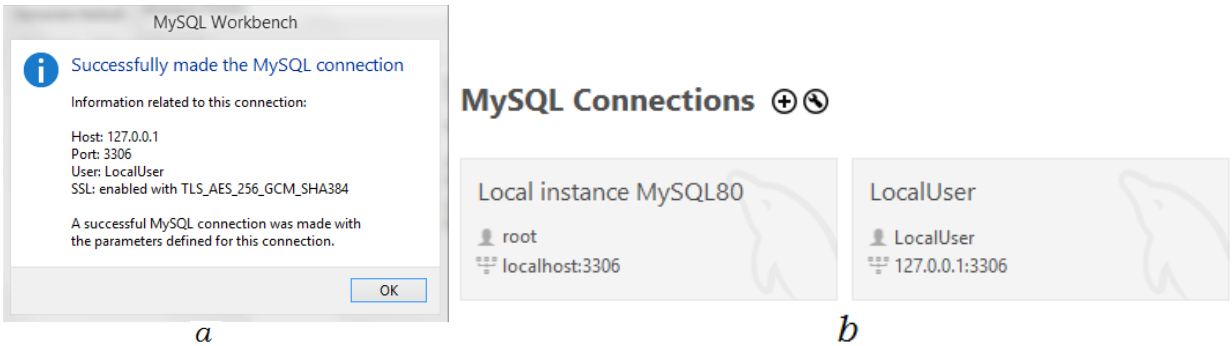


Рис. 5.14. Настройка ManageServerConnections

После чего настройка нового соединения будет успешно завершена (Рис. 15a), а в утилите «MySQLWorkbench» появится новое доступное соединение за нашего созданного непривилегированного пользователя (Рис.5.15b):



a *b*

Рис. 5.15. Завершение настройки нового соединения (a), добавление нового соединения на панель доступных соединений (b)

Попробуем подключиться к серверу с использованием этого нового соединения, выполнив следующие действия: *Кликнуть на подключение LocalUser правой кнопкой мыши → StartCommandLineClient*

Как можно заметить, подключение прошло успешно (рис.5.16):

```
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 23
Server version: 8.0.18 MySQL Community Server - GPL

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| laboratorywork3    |
+--------------------+
2 rows in set (0.00 sec)
```

Рис. 5.16. Успешное подключение пользователя LocalUser к серверу

Очевидно, что непривилегированный пользователь успешно получил доступ к серверу с помощью утилиты «MySQLWorkbench».

5.2.3.2. Назначение специальных прав доступа для пользователя MySQL

В процессе настроек сервера «MySQLServer» была пропущена возможность создания нового пользователя с заданными правами. Используем ее при выполнении данного этапа задания. MySQL позволяет назначать права доступа с помощью следующей команды:

GRANT [*тип прав*] ON [*имя базы данных*].[*имя таблицы*] TO '*имя пользователя*'@'*тип доступа на сервер*';

Нужно заменить значение «тип прав» на тот вид прав доступа, который вы хотите предоставить новому пользователю. Также вам нужно

указать базу данных и имена таблиц, доступ к которым предоставляется. В MySQL есть несколько типов прав доступа, некоторые из них описаны ниже:

- **CREATE** – Позволяет пользователям создавать базы данных/таблицы
- **SELECT** – Позволяет пользователям делать выборку данных
- **INSERT** – Позволяет пользователям добавлять новые записи в таблицы
- **UPDATE** – Позволяет пользователям изменять существующие записи в таблицах
- **DELETE** – Позволяет пользователям удалять записи из таблиц
- **DROP** – Позволяет пользователям удалять записи в базе данных/таблицах

Разрешим пользователю только просмотр записей остальных баз данных, имеющихся в файловой системе SQL: их изменение недопустимо для обычного непривилегированного пользователя, потому что может привести к искажению и даже потере важных данных, как уже упоминалось выше. Сделаем это следующей командой (рис.5.17):

- grant SELECT on *.* to ‘LocalUser’@’loclhost’;

```
mysql> grant SELECT, INSERT on laboratoryWork3.* to 'LocalUser'@'localhost';
Query OK, 0 rows affected (0.07 sec)
```

Рис. 5.17. Назначение прав пользователю LocalUser

Предположим, что АРМ, за которым работает пользователь, расположено в «закрытом» контуре и на нем обрабатываются важные данные. Поскольку в предыдущем задании была создана таблица-телефонный справочник, логично предположить, что пользователь АРМ оперирует данными, предположим, клиентов предприятия. Следовательно, ему можно разрешить права **SELECT**, делать выборку из всех записей таблицы (с целью поиска определенного человека, например, и уточнения его личных данных), и **INSERT**, право на добавление новых записей (если потребуется клиентскую базу). Однако, пользователю нельзя разрешать создавать новые таблицы, модифицировать уже имеющиеся записи и тем более удалять записи и таблицы из базы данных – это может привести к потере важных данных и, как следствие, к потере ресурсов. В случае, если пользователем будет совершена ошибка, ему следует обратиться к администратору (root) базы данных предприятия.

Установим права **SELECT** и **INSERT** на базу данных laboratoryWork3 и непосредственно для таблицы phoneNumbers для пользователя LocalUser следующими командами (рис.5.18):

- grant SELECT, INSERT on laboratoryWork3.* to ‘LocalUser’@’loclhost’;
- grant SELECT, INSERT on laboratoryWork3.phoneNumbers to ‘LocalUser’@’loclhost’;

```
mysql> grant SELECT, INSERT on laboratoryWork3.* to 'LocalUser'@'localhost';
Query OK, 0 rows affected (0.13 sec)

mysql> grant SELECT, INSERT on laboratoryWork3.phoneNumbers to 'LocalUser'@'loca
lhost';
Query OK, 0 rows affected (0.08 sec)
```

Рис. 5.18. Назначение прав пользователю LocalUser

В таблице phoneNumbers пользователь LocalUser имеет право просматривать любые поля и записи, поскольку в соответствии с его ролью на предприятии он оперирует этими данными, поэтому ограничения на доступ к отдельным полям таблицы устанавливать не нужно.

Теперь проверим, применились ли права, просмотрев их для пользователя с помощью команды (рис.5.19):

- show grants for 'LocalUser'@'localhost';

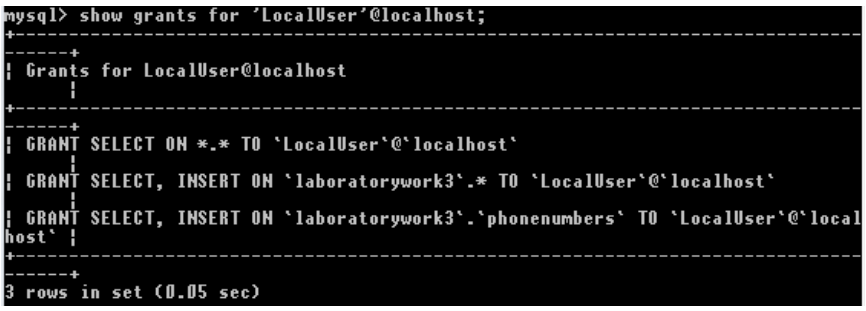


Рис. 5.19. Просмотр прав пользователя LocalUser

Очевидно, что изменение прав доступа к базе данным и содержащимся в них таблицам для пользователя LocalUser успешно осуществлено в соответствии с ролью пользователя на предприятии.

5.2.4. Создание таблицы в ранее установленной базе данных

Создадим пользовательскую таблицу с названием phoneNumbers и с параметрами, заданными в соответствии с условиями лабораторной работы: UserName – тип данных Text, UserAddress – тип данных Text, UserPhone – тип данных Text. Также добавим дополнительную колонку, в которой пропишем автоматический счетчик записей auto_incrementprimarykey типа Integer – это значение будет увеличиваться с каждой новой записью и позволит более гибко оперировать содержимым таблицы. Для этого используем команду (рис.5.20):

- create table phoneNumbers (id integer auto_increment primary key, UserName text not null, UserAddress text not null, UserPhone text not null);

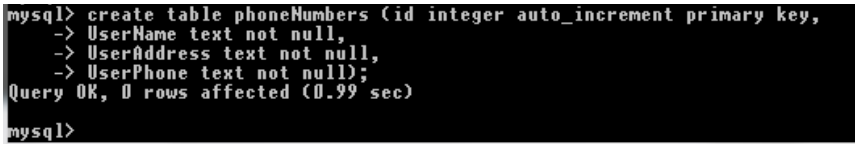


Рис. 5.20. Создание таблицы с заданными колонками

Поскольку сейчас таблица пустая, заполним ее произвольными данными – в нашем примере это телефонная книга, поэтому добавим в нее записи, содержащие имя, адрес и телефонный номер абонентов с помощью команды (рис.5.21):

- insert into phoneNumbers (UserName, UserAddress, User Phone) values (‘Tom’, ‘Alabaevast., 43’, ‘777-88-99’);

```
mysql> insert into phoneNumbers (UserName, UserAddress, UserPhone) values
    -> (’Tom’, ’Alabaeva st., 43’, ’777-88-99’);
Query OK, 1 row affected (0.27 sec)

mysql> insert into phoneNumbers (UserName, UserAddress, UserPhone) values
    -> (’Arina’, ’Rapova st., 18’, ’459-96-32’);
Query OK, 1 row affected (0.18 sec)

mysql> insert into phoneNumbers (UserName, UserAddress, UserPhone) values
    -> (’Kirill’, ’Cherepanova st., 141’, ’123-45-67’);
Query OK, 1 row affected (0.09 sec)

mysql> insert into phoneNumbers (UserName, UserAddress, UserPhone) values
    -> (’Lena’, ’Karimova st., 56’, ’986-54-74’);
Query OK, 1 row affected (0.31 sec)

mysql> insert into phoneNumbers (UserName, UserAddress, UserPhone) values
    -> (’Edvard’, ’Lenina st., 78’, ’223-22-22’);
Query OK, 1 row affected (0.12 sec)
```

Рис. 5.21. Добавление записей в таблицу phoneNumbers

Просмотрим содержимое таблицы. Поскольку команды с show обращаются к файловой системе, необходимо извлечь все столбцы и строки созданной нами таблицы phoneNumbers, что можно сделать следующей командой с использованием ключевого слова select (рис.5.22):

- select * fromphoneNumbers;

```
mysql> select * from phoneNumbers;
+----+----------+---------------------+-----------+
| id | UserName | UserAddress         | UserPhone |
+----+----------+---------------------+-----------+
|  1 | Tom      | Alabaeva st., 43    | 777-88-99 |
|  2 | Arina    | Rapova st., 18      | 459-96-32 |
|  3 | Kirill   | Cherepanova st., 141 | 123-45-67 |
|  4 | Lena     | Karimova st., 56    | 986-54-74 |
|  5 | Edvard   | Lenina st., 78      | 223-22-22 |
+----+----------+---------------------+-----------+
5 rows in set (0.00 sec)
```

Рис. 5.22. Просмотр содержимого таблицы phoneNumbers

Очевидно, что новая таблица phoneNumbers с несколькими записями успешно создана.

5.2.4.1. Запрос выборок из таблицы

Проверим корректность настроенных прав для пользователя LocalUser, а также ознакомимся с механизмом запроса записей из таблицы в SQL.

Сделаем несколько выборок из таблицы phoneNumbers:

1) Выборка из таблицы phoneNumbers значений адреса и телефона для пользователей 'Tom' и 'Edvard' с помощью следующих команд (рис.5.23):

- select UserAddress, UserPhone from phoneNumbers where UserName=’Tom’;
- select UserAddress, UserPhone from phoneNumbers where UserName=’Edvard’;

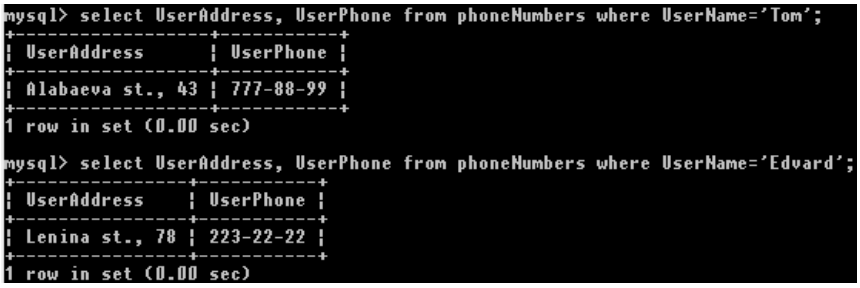


Рис. 5.23. Результат выборки по значениям адреса и телефона для двух произвольных пользователей

2) Выборка всех записей из таблицы phoneNumbers с сортировкой по полю UserName в алфавитном порядке с использованием следующей команды (рис.5.24):

- select * from phoneNumbers order by UserNameasc;

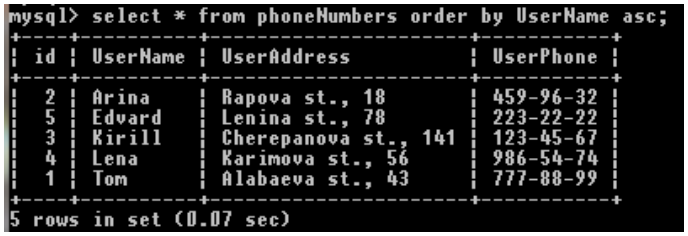


Рис. 5.24. Результат выборки по всем записям в алфавитном порядке

Очевидно, что запросы пользователя LocalUser к таблице phoneNumbers успешно выполняются.

3) Проверим, корректно ли работает механизм задания прав пользователя, попробовав удалить таблицу phoneNumbers с использованием следующей команды (рис.5.25):

- drop table phoneNumbers;

Рис. 5.25. Попытка удаления таблицы пользователем LocalUser, у которого нет на это прав

Очевидно, что пользователю LocalUser действительно не хватает прав на удаление таблицы phoneNumbers – как и настраивалось ранее. Следовательно, механизм безопасности на основе прав доступа к базе данных и таблице работает правильно.

5.2.4.2. Удаление таблиц, баз данных и пользователей

На последнем этапе рассмотрим механизм удаления таблиц, баз данных и пользователей из файловой системы SQL. Это можно сделать только привилегированным-root пользователем, поэтому дальнейшая работа будет осуществляться из его терминала.

1) Удаление таблицы phoneNumbers из базы данных laboratoryWork3. Содержимое базы данных до удаления таблицы (рис.5.26):

```
mysql> use laboratoryWork3;
Database changed
mysql> show tables;
+---------------------------+
| Tables_in_laboratorywork3 |
+---------------------------+
| phonenumbers              |
+---------------------------+
1 row in set (0.10 sec)
```

Рис. 5.26. Содержимое базы данных laboratoryWork3 до удаления таблицы phoneNumbers

Удалим таблицу phoneNumbers с помощью команды (рис.5.27):

- drop table phoneNumbers;

```
mysql> drop table phoneNumbers;
Query OK, 0 rows affected (0.24 sec)

mysql> show tables;
Empty set (0.00 sec)
```

Рис. 5.27. Содержимое базы данных laboratoryWork3 после удаления таблицы phoneNumbers

2) Удаление базы данных laboratoryWork3. Список баз данных до удаления (рис.5.28):

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| laboratorywork3    |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)
```

Рис. 28. Список всех баз данных в файловой системе SQL до удаления базы данных laboratoryWork3

Удалим таблицу phoneNumbers с помощью команды (рис.5.29):

- drop database laboratoryWork3;

```
mysql> drop database laboratoryWork3;
Query OK, 0 rows affected (0.13 sec)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.00 sec)
```

Рис. 5.29. Список всех баз данных в файловой системе SQL после удаления базы данных laboratoryWork3

3) Удаление всех прав доступа пользователя LocalUser с помощью следующей команды (рис.5.30):

- revoke all privileges on *.* from ‘LocalUser’@’localhost’;

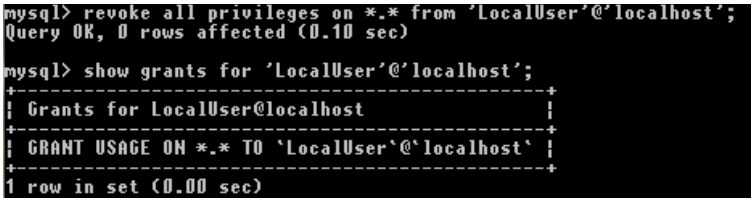


Рис. 5.30. Удаление прав пользователя LocalUser и проверка корректности выполнения команды

4) Удалим пользователя LocalUser. Посмотрим список всех пользователей до удаления LocalUser, обратившись к таблице mysql.user и запросив из нее всех пользователей и их способ подключения к серверу с помощью команды (рис.5.31):

- select User, Host from mysql.user;

Рис. 5.31. Список имеющихся пользователей до удаления LocalUser

Удалим пользователя LocalUser с помощью команды (рис.5.32):

- drop user 'LocalUser'@'localhost';

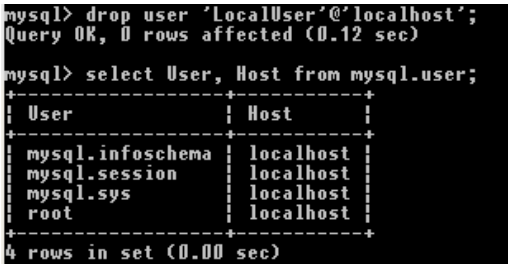


Рис. 5.32. Список имеющихся пользователей после удаления LocalUser

Очевидно, что удаление баз данных, пользователей и таблиц успешно осуществлено.

Выводы по лабораторной работе

В работе проведена установка MySQL, создана база данных. Назначены и проверены права пользователя по доступу к ресурсам севера базы данных. Настройка параметров безопасности с учетом принятой политики информационной безопасности в организации - прав доступа к ресурсам севера базы данных, а именно, SELECT, права на выборку из всех записей таблицы (с целью поиска определенного человека, например, и уточнения его личных данных), и INSERT, право на добавление новых записей (если потребуется клиентскую базу) позволяет повысить уровень защиты базы данных от НСД.

6. Содержание отчета

6.1. Цель работы

6.2. Теоретические сведения

6.3. Процесс установки MySQL и создания новой базы данных, а также пользователя MySQL.

6.4. Процесс создания и структуру таблицы в базе данных (телефонный справочник, каталог книг, перечень товаров на складе и др.)

6.5. Обосновать критерии выбора настроек и настройкудоступа из клиента базы данных (программы mysql.exe) по доступу к управлению сервером и к отдельным таблицам и полям таблиц, а также встроенным функциям и хранимым процедурам.

6.6. Описать работу пользователя с таблицей с учетом настроенных параметров безопасности и их проверку.

6.7. Указать последовательность команд SQL, используемую при выполнении задания, с комментариями по каждой команде, а также ответы сервера.

6.8. Сформулировать выводы.

7. Контрольные вопросы

7.1. Для чего используется язык SQL?

7.2. Какие разновидности баз данных вы знаете?

7.3. Как строятся реляционные базы данных?

7.4. Как характеризуют MySQL её разработчики?

7.5. На чем основана система безопасности MySQL?

7.6. Какие параметры входят в систему привилегий (privilegesystem)?

7.7. Как происходит процесс установки и администрирования сервера MySQL

7.8. Как настраиваются параметры доступа из клиента базы данных (программы mysql.exe) к управлению сервером и к отдельным таблицам и полям таблиц, а также встроенным функциям и хранимым процедурам?

ЛАБОРАТОРНАЯ РАБОТА 4
«НАСТРОЙКА ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ АРМ»

1. Цель работы

Изучить и научиться настраивать изолированную программную среду (ИПС) на автономном автоматизированном рабочем месте (АРМ) пользователя средствами операционной системой Windows для защиты информации от несанкционированного доступа (НСД).

Используемое программное обеспечение: ОС Windows 7 или более старшие версии.

2. Задание к лабораторной работе

2.1. Провести редактирование ключей реестра раздела Explorer для ограничения функционала рабочего стола и меню «Пуск» пользователя.

2.2. Отредактировать реестр для ограничения функционала «Панели управления».

2.3. Отредактировать реестр для закрытия меню «Пуск» от редактирования.

2.4. Сформулировать выводы

3. Теоретические сведения

Windows обладает достаточно обширным набором функций и утилит для изменения конфигурации и подключения новых устройств и ресурсов. С одной стороны, эти функции облегчают работу квалифицированному пользователю, но с другой - могут служить источником несанкционированного доступа (НСД). Защита информации от несанкционированного доступа НСД на каждом АРМ осуществляется индивидуально с учетом решаемых на нем задач и включает, в том числе, настройку изолированной (замкнутой) программной среды (ИПС) средствами ОС Windows.

Изолированная программная среда ИПС АРМ предназначена для ограничения возможностей пользователя по запуску программ, доступу к файлам, изменению параметров операционной системы (ОС). Настройка замкнутой программной среды обеспечивает возможность запуска только заданного набора программ и/или процессов для пользователя, т.е. исключает

возможность запускать ему собственные, не разрешенные явно администратором, задачи.

Механизм ИПС позволяет сформировать для любого пользователя компьютера программную среду, определив индивидуальный перечень программ, разрешенных для запуска. Перечень программ, разрешенных для запуска, может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей.

Организация ИПС средствами ОС Windows осуществляется сокрытием от пользователя части элементов интерфейса путём присвоения параметрам реестра ОС определенных значений (например, скрытие элементов рабочего стола, скрытие пункта меню «Выполнить» кнопки «Пуск», запрет контекстного меню кнопки «Пуск», запрет контекстного меню для «Панели задач» и др.). При этом параметры реестра различных версий ОС Windows могут значительно различаться.

Редактор реестра в Windows является своеобразным «хранилищем» системы, которое содержит в себе настройки и параметры, как самой операционной системы, так и различных программ, установленных в ней, а также многого другого, необходимого для работы Windows.

Редактор реестра содержит список его главных разделов (rootkeys, корневых ключей). Внутри них содержатся все значения реестра. Ниже приведен список с наиболее распространенными разделами и их содержимым (значениями).

- HKEY_CLASSES_ROOT (HKCR) – раздел, содержащий типы файлов, их расширения и OLE информацию.
- **HKEY_CURRENT_USER (HKCU)** – раздел, содержащий настройки текущего пользователя, вошедшего в Windows. Именно с ним осуществляться работа по настройке ППС.
- HKEY_LOCAL_MACHINE (HKLM) – раздел, содержащий конкретную информацию об установленном оборудовании, настройках программного обеспечения и другую информацию. Эти настройки используются для всех пользователей компьютера.
- HKEY_USERS (HKU) – раздел, содержащий информация обо всех пользователях компьютера (профилях).
- HKEY_CURRENT_CONFIG (HKCC) – раздел, содержащий подробности о текущей конфигурации аппаратных средств компьютера.

Структура реестра Windows строго иерархична и имеет четкое построение. Основная его составная часть – это ***ключи (или параметры)***, в которых и хранится вся информация (в нашем примере это ключ с названием ***«link»).*** Каждый параметр реестра Windows отвечает за определенное свойство системы. Ключи с данными о смежных настройках компьютера объединены в разделы, которые, в свою очередь, являются подразделами более крупных разделов и т.д.

Параметры (ключи) реестра бывают нескольких видов (***параметры DWORD, QWORD, двоичные, строковые и многострочные параметры и***

др.) в зависимости от сведений, которые в них содержатся. Информацию с этих ключей Windows считывает главным образом во время запуска, поэтому для того чтобы внесенные в реестр Windows изменения вступили в силу, нужно перезагрузить компьютер.

РазделExplorer, в который необходимо вносить изменения, отвечает за настройки экрана, рабочего стола и т.д.Создание раздела Explorerпроизводится через свойства раздела Policies.

Изменения в реестр вносятся путем создания определенных ключей и задания им нужных параметров, чтобы в результате была установлена ИПС.

Всего реестр позволяет выбирать из пяти типов параметров:

- REG_BINARY — тип двоичных параметров (BinaryValue), которые представляют собой набор двоичных данных, доступных для редактирования только в шестнадцатеричном формате.
- REG_DWORD — тип параметра, имеющий числовое значение (DWORD Value), которое может задаваться либо в десятичном, либо в шестнадцатеричном формате.
- REG_SZ — тип параметра, значение которого задается в виде текстовой строки (StringValue) фиксированной длины. Как правило, данный тип параметра содержит текст, который можно прочитать.
- REG_EXPAND_SZ — тип параметра, значение которого задается в виде строки данных переменной длины (ExpandableStringValue). Этот тип данных включает имена специальных переменных, обрабатываемых при использовании данных программой или службой. Когда программа или служба читает такую строку из реестра, то операционная система автоматически подставляет вместо имени специальной переменной ее текущее значение.
- REG_MULTI_SZ — тип параметра, значение которого задается в виде многострочного текста (Multi-StringValue). К такому типу, как правило, относятся списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами.

Для применения параметра необходимо изменитьустановленное по умолчанию значение параметра «0» на «1».

После того, как все параметры добавлены, можно экспортировать всю директорию Explorer в отдельный файл, для удобства работы с реестром путем редактирование отдельного файла.

3.1. Последовательность выполнения лабораторной работы

4.1. Повести редактирование ключей реестра раздела Explorer для ограничения функционала рабочего стола и меню «Пуск» пользователя
4.2. Осуществить экспорт директории Explorer
4.3. Провести анализ изменений меню «Пуск»
4.4. Отредактировать реестр для ограничения функционала «Панели управления».
4.5. Отредактировать реестр для закрытия меню «Пуск».

4.6. Сформулировать выводы

3.2. Методические указания по выполнению работы

Для того, чтобы можно было наглядно проследить изменения, которые вносит ИПС, ниже приведены изображения внешнего вида рабочего стола (рис.5.1) и окна «Пуск» (рис.5.1) для некоторого АРМ до применения изменений ИПС.

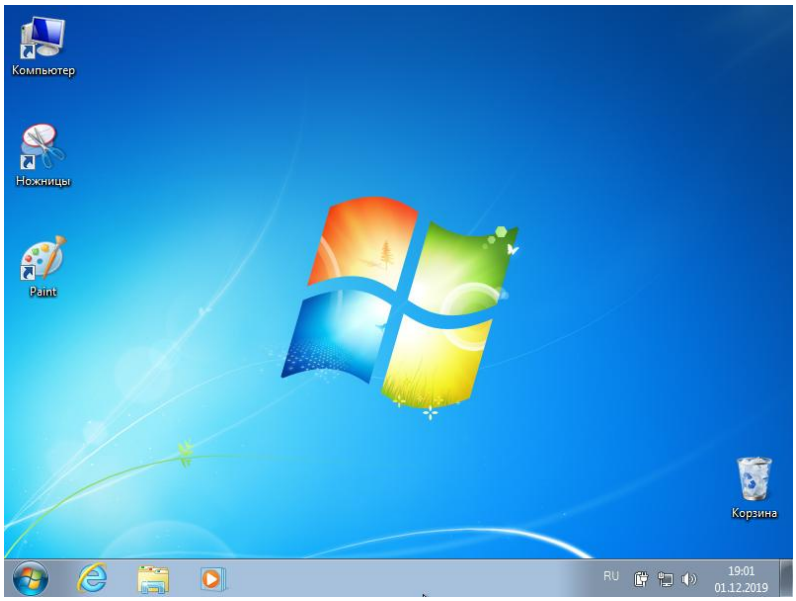


Рис.5. 1. Рабочий стол до установки на АРМ ИПС

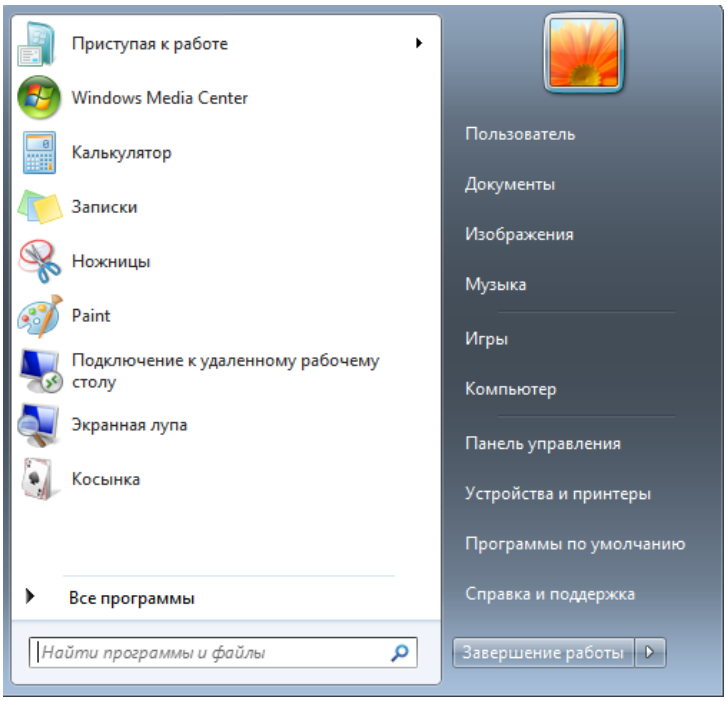


Рис.5. 2. Меню «Пуск» до установки на АРМ ИПС

Для создания ИПС на АРМ можно использовать два подхода:

1. Замещение пользовательской оболочки собственной задачей, которая предлагает замкнутое меню (этот путь достаточно тривиален и предусматривает написание простого оконного приложения и указания пути к нему в ключе Shell).
2. Задание ключей реестра, позволяющих ограничить число задач в меню Пуск стандартной оболочки.

Далее будет рассматриваться второй вариант, с использованием ключей реестра, выбираемых в соответствии с заданием на лабораторную работу.

5.1. *Перейти в редактор реестра*

Для редактирования параметров реестра, требуется сначала перейти в редактор реестра. Для этого нужно нажать сочетание клавиш Win+R или в меню Пуск найти пункт «Выполнить», после чего в открывшемся окне ввести команду «regedit» и нажать ОК.

Чтобы открыть редактор реестра нужно открыть окно пункта меню «Выполнить» кнопки «Пуск» сочетанием клавиш *Win+R*, а после ввести *«regedit»* в окно поиска (рис.5.3):

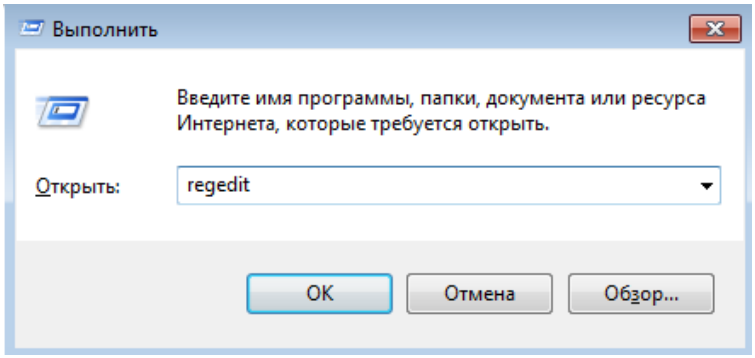


Рис. 5.3. Окно пункта меню «Выполнить» кнопки «Пуск»

После чего откроется окно редактора реестра (рис.5.4):

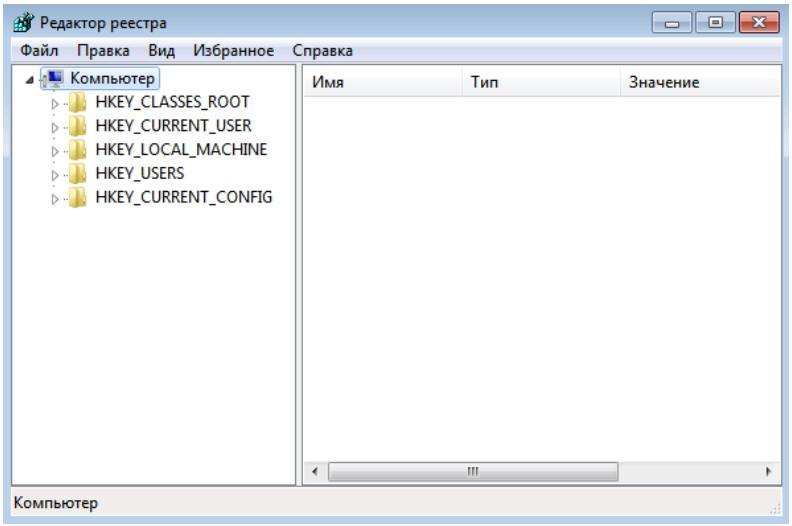


Рис. 5.4. Главное окно редактора реестра

5.2. *Перейтивраздел Policies*

Реестр имеет иерархическую структуру, которая напоминает файловую систему жесткого диска – с его каталогами, подкаталогами и файлами. Но называются элементы реестра по-другому: верхний уровень иерархии составляют разделы, каждый из которых может содержать вложенные подразделы, а также параметры. Именно в параметрах хранится основное содержимое реестра, разделы служат лишь для группировки схожих по назначению параметров.

При входе в редактор реестра можно увидеть список его главных разделов (rootkeys, - корневых ключей). Внутри них содержатся все значения реестра. Для того, чтобы открыть раздел достаточно просто перемещаться по соответствующим папкам дерева каталогов, отображаемого в левой части окна редактора реестра. Вданномокнеперейдемвраздел *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies*,
Искомый раздел выглядит следующим образом (рис.5.5):

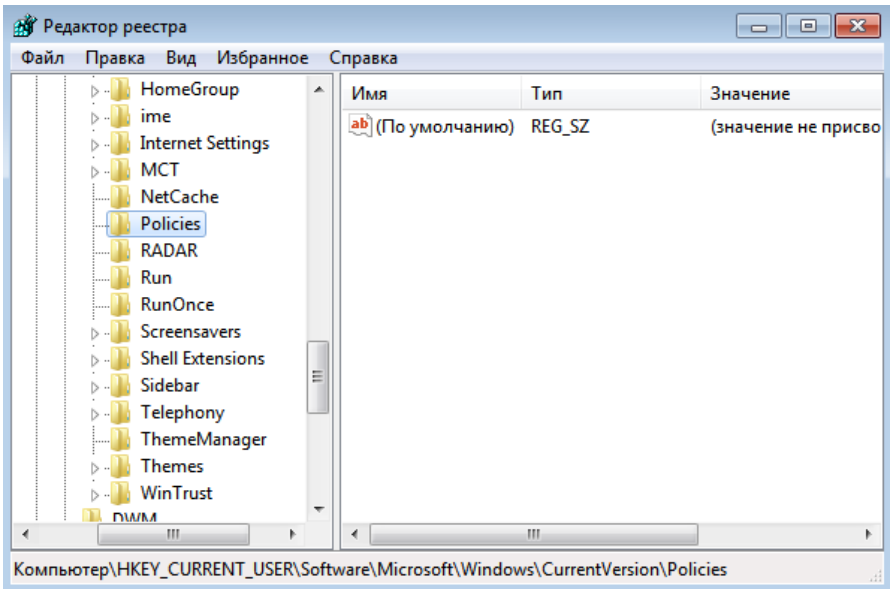


Рис. 5.5. Раздел настроек текущего пользователя, категория настроек локальных политик

5.3. *Создать раздел Explorer*

В кусте реестра HKEY_CURRENT_USER хранятся папки пользователя, цвета экрана и параметры панели управления. Эти сведения сопоставлены с профилем пользователя. Вместо полного имени раздела иногда используется аббревиатура HKCU. Как можно заметить в этом разделе ещё отсутствует раздел Explorer, в который необходимо вносить изменения: этот раздел отвечает за настройки экрана, рабочего стола и т.д.в который необходимо вносить изменения. Поэтому следующий шаг – создание раздела Explorer.

Для того, чтобы создать новый раздел, следует кликнуть правой кнопкой мыши (ПКМ) по родительскому разделу и в контекстном меню выбрать сначала пункт «Создать», а потом «Раздел», т.е. создание раздела производится через свойства раздела Policies следующим образом: *выделить раздел Policies → ПКМ → Создать → Раздел → Explore*r. Этапы создания показаны на рисунке ниже (рис.5.6):

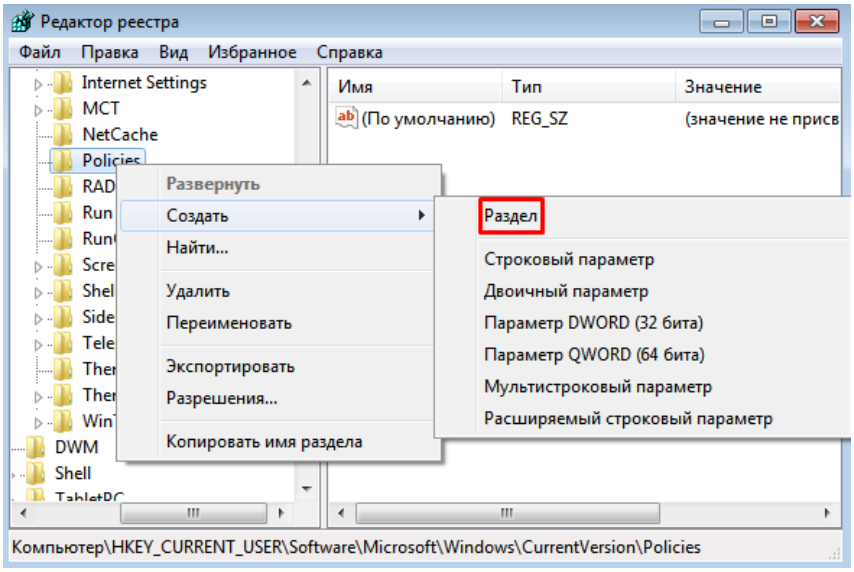


Рис. 5.6. Создание раздела Explorer

После этого требуется ввести название нового раздела и готово – раздел создан.В результате будет добавлен нужный нам раздел. Сейчас он пуст, в нем нет никаких ключей, кроме ключа по умолчанию, и выглядит он следующим образом (рис.5.7):

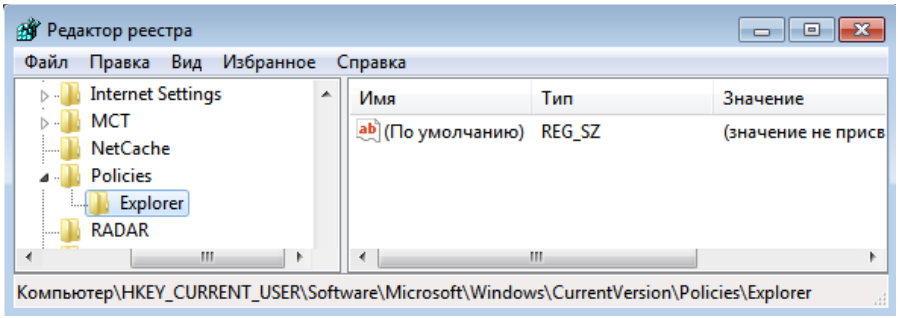


Рис. 5.7. Раздел Explorer

5.4. *Создать параметр NoDesktop*

Раздел и подраздел могут быть пустыми или содержать один, или несколько параметров, параметр по умолчанию. Каждый параметр имеет имя, тип и значение. Три части параметра реестра всегда располагаются в определенном порядке: имя, тип данных, значение.

Для организации ИПС на АРМ внесем изменения в разделExplorer-создадим определенные ключи и зададим им определенные значения параметров. Для начала создадим в разделе Explorer новыйпараметр типа DWORD через контекстное меню. Данные типа DWORD – это данные,

представленные целым числом (4 байта, 32 бита). Многие параметры служб и драйверов устройств имеют этот тип и отображаются в двоичном, шестнадцатеричном или десятичном форматах. Присвоим имя созданному параметру – NoDesktop, и установим его значение равным «1». Этот параметр позволяет скрыть все элементы («ярлыки») на рабочем столе.Данная мера ограничивает действия пользователя вустановке лишних ярлыков на рабочем столе.

Этапы создания показаны на рисунке ниже (рис.5.8):*выделить раздел реестра Explorer → ПКМ → Создать → Параметр DWORD (32 бита)*.

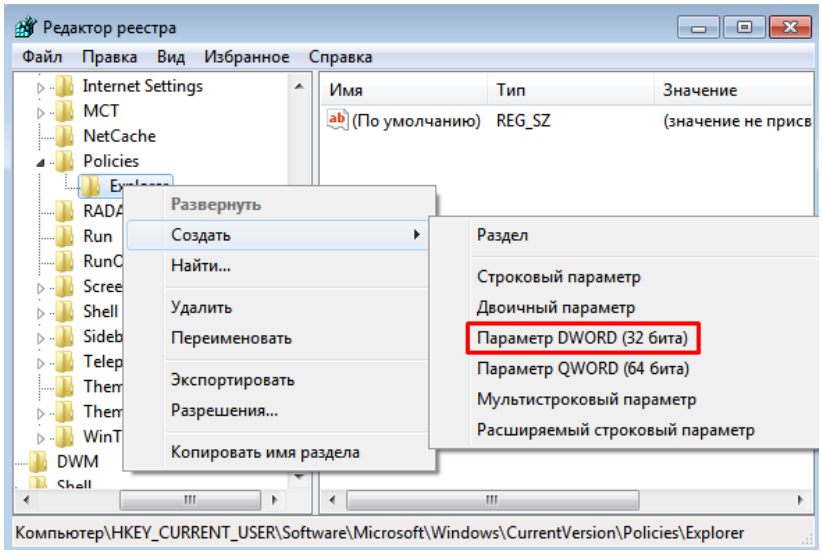


Рис. 5. 8. Создание параметра NoDesktop

В результате будет создан новый параметр с заданным именем, с выбранным типом и со значением «0», поскольку параметр при создании инициализируется именно им. В случае параметра NoDesktop со значением «0» означает отображение ярлыков (рис.5.9):

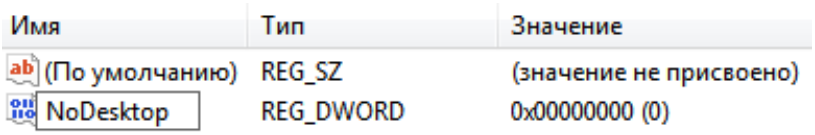


Рис. 5.9. Значение созданного параметраNoDesktop

Поскольку цель применения параметра: скрыть отображение значков и ярлыков рабочего стола для пользователя, изменим значение по умолчанию параметра «0» на «1» (рис.5.10). Делается это следующим образом: *выделить параметр NoDesktop → дважды щелкнуть на нем ЛКМ → установить значение параметра в «1»*.

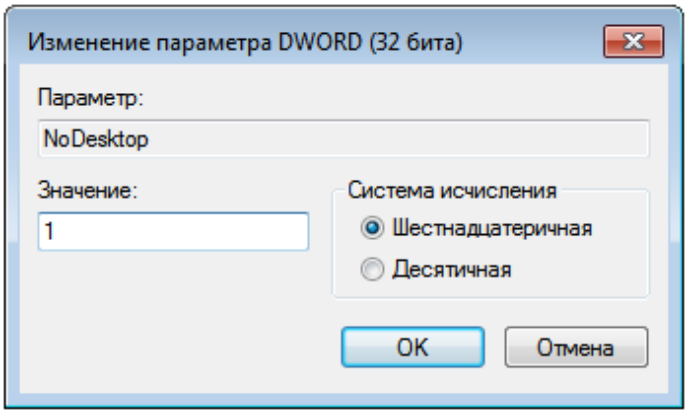


Рис. 5.10. Изменение значения параметра NoDesktop

После внесения изменений параметр будет отображаться следующим образом (рис.5.11):

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
NoDesktop	REG_DWORD	0x00000001 (1)

Рис. 5.11. Значение параметра NoDesktop после изменений

5.5. **Перезагрузить машину**

В большинстве случаев, для того, чтобы изменения, внесенные в реестр, вступили в силу, нужна перезагрузка или выход и повторный вход в систему. Перезагрузим АРМ и посмотрим, как отобразятся внесенные нами ранее изменения (рис.512).

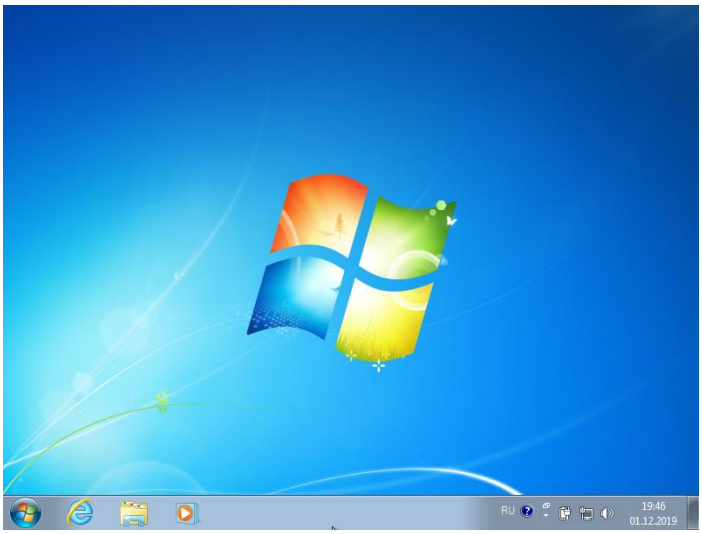


Рис. 12. Рабочий стол после внесения изменений

С рабочего стола исчезли все ярлыки, а также на рабочем столе не работает контекстное меню (нажатие ПКМ не получают отклика). Однако, посмотреть содержимое все еще возможно через функционал «Проводник» (рис.5.13):

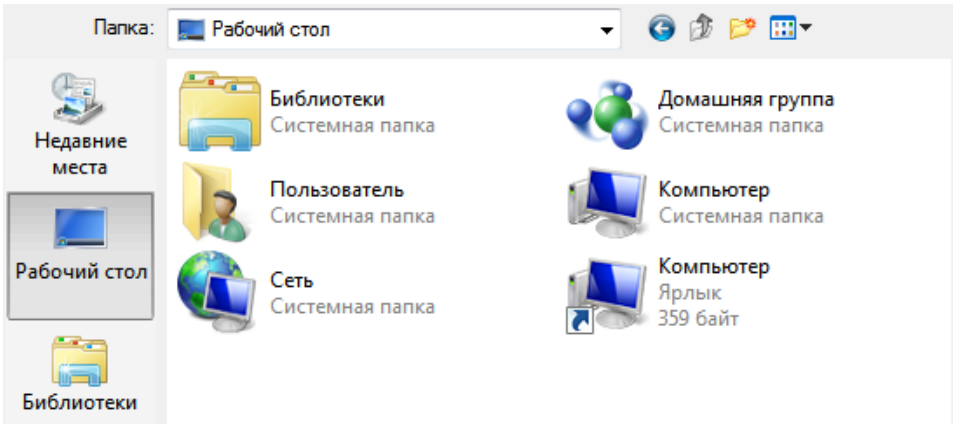


Рис. 5.13. Содержимое рабочего стола

Следовательно, ключ реестра NoDesktop не удаляет ярлыки и значки с рабочего стола пользователя, но запрещает их отображение. Очевидно, что пользователь не может редактировать содержимое рабочего стола, а также выносить на него свои ярлыки.Проделаем аналогичную работу с другими параметрами.

5.6. *Добавить остальные параметры реестра для организации ИПС*

Как уже было сказано, организация ИПС средствами ОС Windows 7 осуществляется сокрытие от пользователя части элементов интерфейса путём присвоения некоторым параметрам реестра ОС, представленным в таблице ниже, определенных значений. Процесс создания новых ключей и присвоения им значений аналогичен пунктам 5.3 – 5.5, поэтому приводится не будет.

Для удобства представим все внесенные изменения в виде табл.5.1.

Таблица 5.1.

Название параметра	**Тип**	**Значение**	**Описание**
NoDesktop	DWORD	1	Скрытие элементов рабочего стола
NoRun	DWORD	1	Скрыть пункт меню «Выполнить» кнопки Пуск
NoFind	DWORD	1	Скрыть пункт меню «Найти» кнопки Пуск
NoRecentDocsMenu	DWORD	1	Скрыть пункт меню «Документы» кнопки Пуск
NoFavoritesMenu	DWORD	1	Скрыть пункт меню «Избранное» кнопки Пуск
NoSetFolders	DWORD	1	Скрытие пунктов меню «Принтеры» и «Панель управления» из меню «Настройка» кнопки Пуск
NoWindowsUpdate	DWORD	1	Скрытие пункта «WindowsUpdate» из меню Настройки кнопки Пуск

NoSetTaskbar	DWORD	1	Скрытие «Панели задач» и меню Пуск из меню «Настройка» кнопки Пуск
NoSetActiveDesktop	DWORD	1	Скрытие пункта «Рабочий стол ActiveDesktop» из меню Настройка кнопки Пуск
NoChangeStartMenu	DWORD	1	Запрет контекстного меню кнопки Пуск
NoRecentDocsHistory	DWORD	1	Очистка недавно открытых документов
ClearRecentDocsOnExit	DWORD	1	Очистка списка недавно открытых документов при выходе
NoTrayContextMenu	DWORD	1	Запрет контекстного меню для Панели задач
NoFolderOptions	DWORD	1	Запрет пункта «Свойства папок» из Меню настройка кнопки Пуск
NoViewContextMenu	DWORD	1	Запрет контекстного меню по правой клавише мыши на Рабочем столе
NoCustomizeWebView	DWORD	1	Запрет настройки вида конкретных папок Меню Вид команда Настроить вид папки

Напомним, что все изменения производятся для раздела реестра: *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer.*

Содержимое раздела Explorer после внесения изменений (рис.5.14):

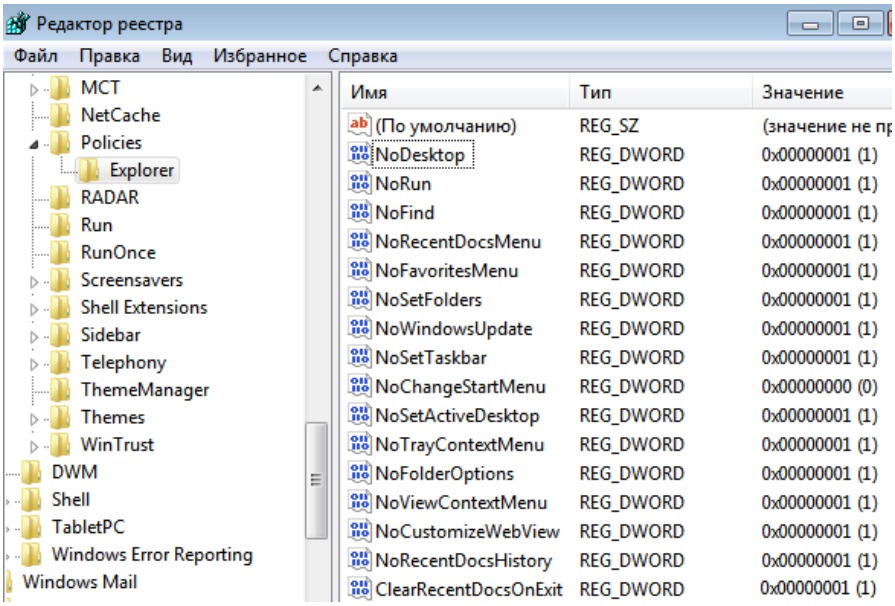


Рис. 5.14. Раздел реестра Explorer после внесения изменений

5.7. *Экспорт директории Explorer*

После того как настроены все выбранные параметры реестра важно сохранить полученные значения в файл, т.к. резервная копия параметров реестра позволит не только вернуться к настроенным параметрам в случае необходимости, но и ускорит процесс настройки других АРМ. Экспорт всей директорииExplorer в отдельный файл позволит не только получить короткий доступ к реестру, нои удобно работать с реестром через редактирование отдельного файла.

Для этого в редакторе реестра необходимо (рис.5.15): *выделить раздел реестра Explorer → в строке меню выбрать Файл → Экспорт… → место сохранения (рис. 5.16).*

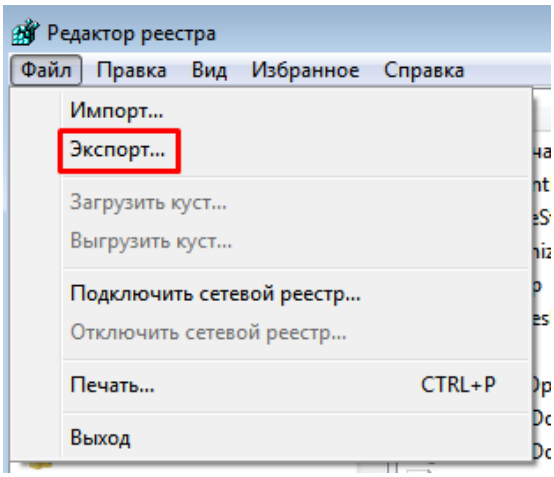


Рис. 5.15. Экспорт директории Explorer

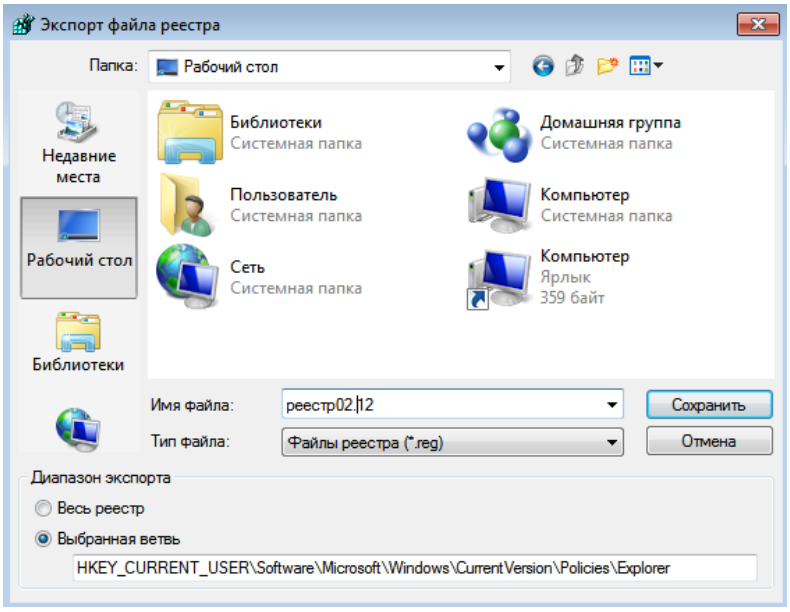


Рис. 5.16. Выбор места сохранения файла реестра

После экспортирования раздела реестра с REG-файлами, которые он содержит, можно работать, как с обычным текстовым файлом, используя для этого стандартные текстовые редакторы (например, «Блокнот»).Содержимое экспортированной файла реестра «реестр02.12.reg», просматриваемое с помощью программы «Блокнот» (рис.5.17):

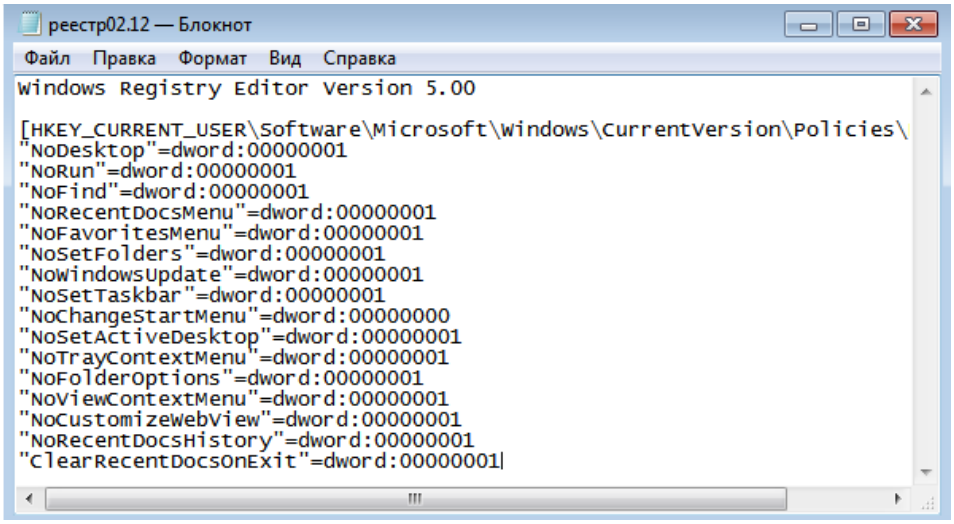


Рис. 5.17. Содержимое файла реестра «реестр02.12.reg»

Для восстановления значения какого-либо раздела реестра по имеющейся заплатке достаточно два раза щелкнуть мышью по REG-файлу — его содержимое будет автоматически добавлено внутрь реестра. Кроме того, при запущенном редакторе реестра можно в его строке меню выбрать Файл → Импорт, а затем указать REG-файл, который требуется импортировать.

5.8. *Анализ изменений меню Пуск*

Проанализируем, как измениться содержимое меню «Пуск» после применения параметров и перезагрузки машины.Смотрим отображение меню «Пуск» до (слева) и после (справа) внесения изменений (рис. 5.18):

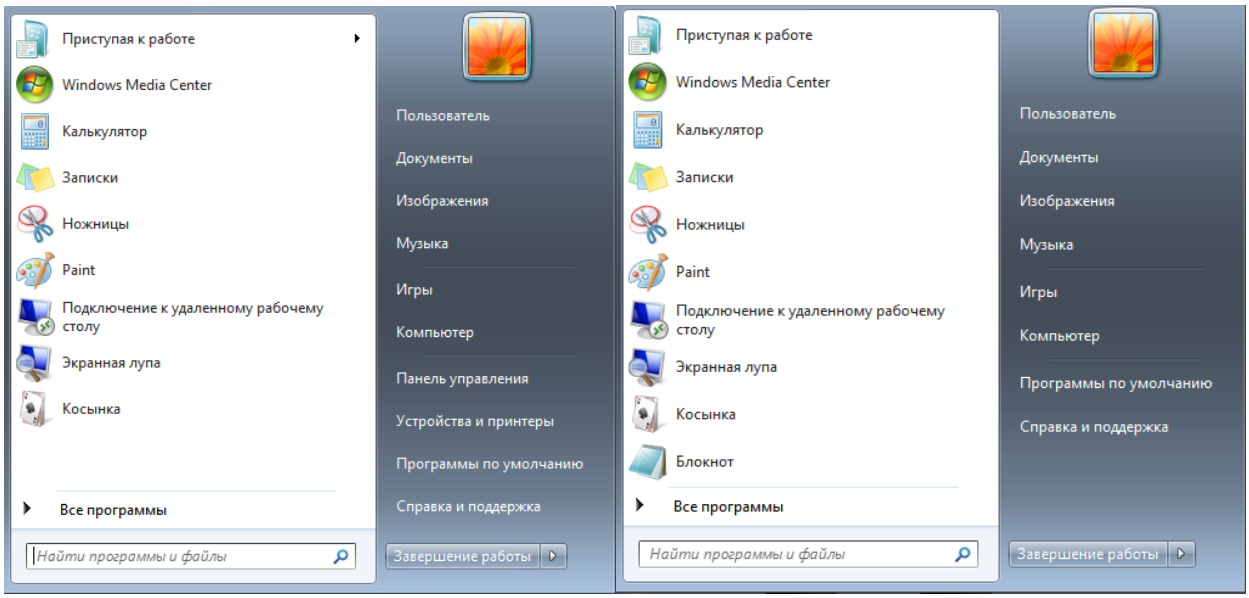


Рис. 5.18. Меню «Пуск» до внесения изменений в реестр (слева) и после (справа)

Проверим результаты применения параметров NoRun - скрыть пункт меню «Выполнить» кнопки Пуск и NoSetFolders- скрытие пунктов меню «Принтеры» и «Панель управления» из меню «Настройка» кнопки Пуск.

До применения параметров существовала возможность запустить редактор реестра через поиск меню «Панель управления» из меню «Настройка» кнопки Пуск и через меню «Выполнить» кнопки Пуск. Проверим недоступность редактора реестра через меню «Панель управления» из меню «Настройка» кнопки Пуск. После применения параметров это осуществитьнельзя (пункт «Выполнить» меню Пускскрыт, а доступ через сочетание клавиш Win+Rприводит к ошибке – результат применения ключа NoRun(рис.5.19)).

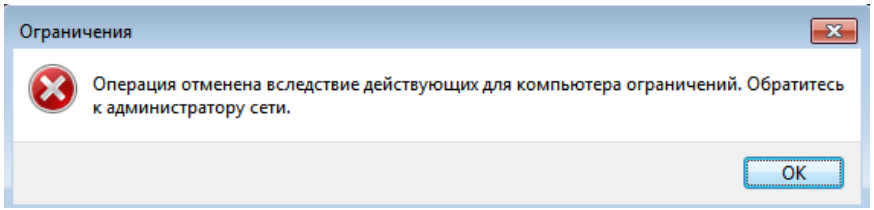


Рис. 5.19. Реакция системы на вызов пункта «Выполнить» меню «Пуск»сочетанием клавиш Win+R

После применения настроек ключа реестра NoSetFolders из поиска нельзя увидеть и зайти в реестр в режим редактирования(рис.5.20). Такой способ защиты информации можно использовать в корпорациях или компаниях, чтобы сотрудники, у которых не должно быть доступа изменения настроек, не смогли этого сделать.

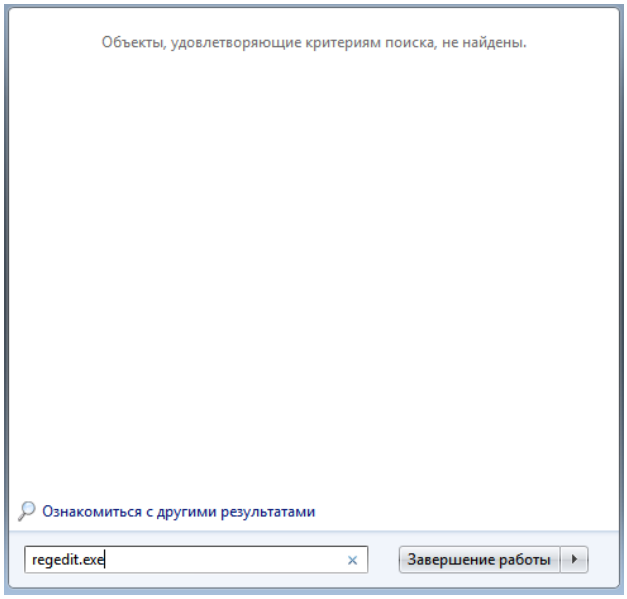


Рис. 5.20. Отключение функционала пункта меню «Панель управления» из меню «Настройка» кнопки Пуск

Также до применения настроек через кнопку Пуск можно было вызвать контекстное меню. После применения параметров реестра это действия стало невозможным, поэтому при нажатии правой клавиши мыши в меню Пуск ничего не происходит.

Однако, при этом следует помнить, что редактор реестра может быть запущен из командной строки Windows, если не принять дополнительных мер защиты. *Открыть тот же редактор реестра можно напрямую запустив его exe-файл, расположенный по адресу C:\Windows\regedit.exe.*Следовательно, можно сделать вывод, что для полного ограничения возможностей пользователя по запуску редактора реестра необходимо также ограничить доступ пользователя к содержимому диска С (рис.5.21).

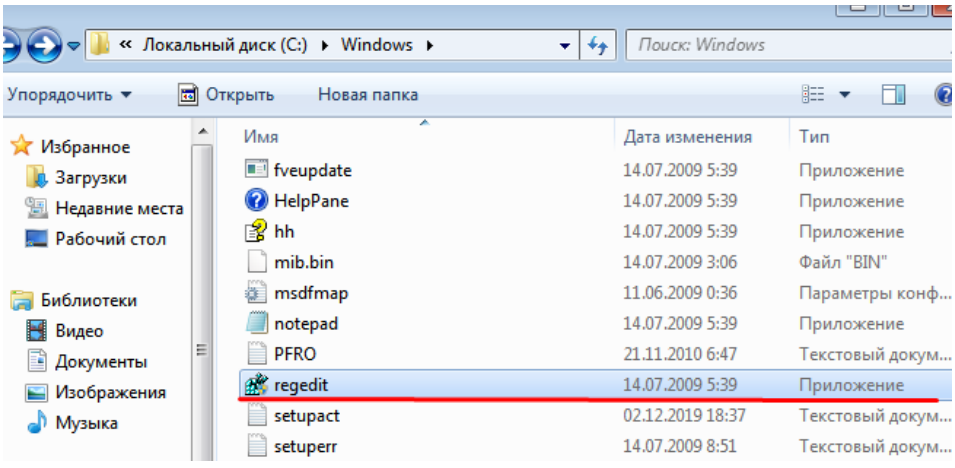


Рис. 5.21. Доступ к редактору реестра через его местоположение

Кроме того, «Панель управления», которая была скрыта из меню «Панель управления» из меню «Настройка» кнопки Пуск доступна через поисковую строку (рис.5.22):

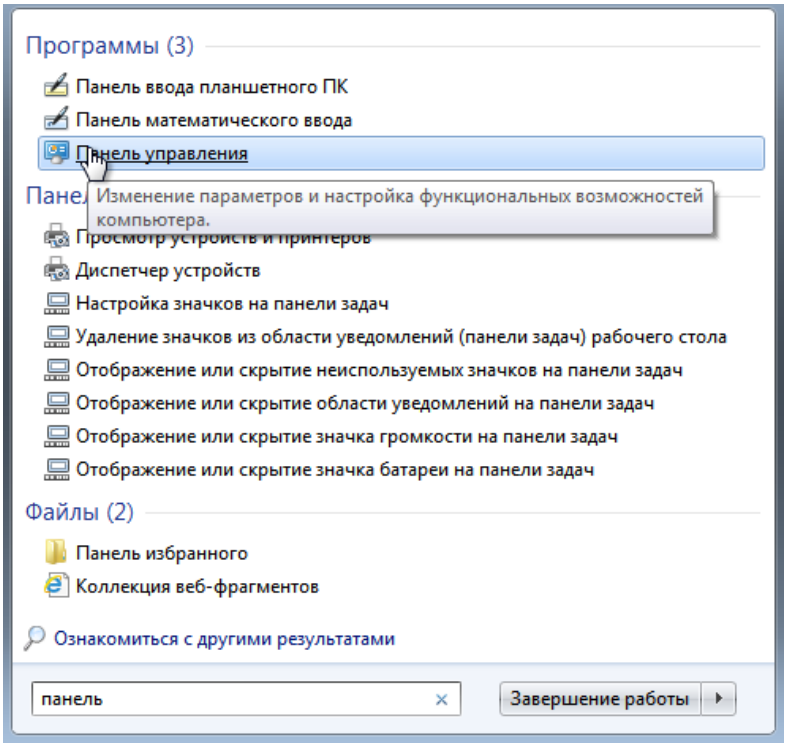


Рис. 5.22. Результат поиска «Панель управления»

5.9. ***Отредактировать реестр для ограничения функционала «Панели управления»***

Поскольку в результате применения предыдущих настроек доступ к самой «Панели управления» у пользователя остался, не смотря на то, что она была скрыта в функционалеменю кнопки Пуск - в целях безопасности ограничим функционал «Панели управления».

В качестве примера заблокируем настройки пункта «Экран» панели управления и заблокируем возможность изменения обоев рабочего стола пункта «Персонализация» панели управления. Первое сделано для удобства пользователя, второе – чтобы пользователь не мог установить на АРМ собственные обои, которые, например, будут включать изображение пароля от какой-то базы данных, с которой работает пользователь (вынесенное на рабочий стол поскольку пользователь не может его запомнить).

Для этого следует создать в директории Policiesновые разделы (рис.5.23) *SystemuActiveDesktop*(полный путь остался прежним):

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\ Policies)разделы System и ActiveDesktop.

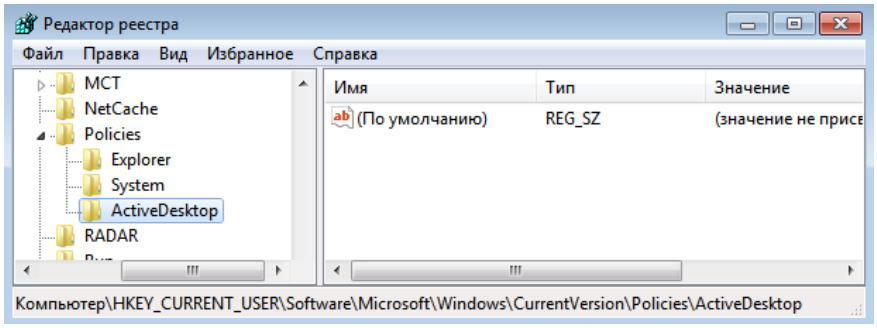


Рис. 5.23. Новые разделы System и ActiveDesktop в директории Policies

Теперь создадим по аналогии пунктов 5.3 – 5.5 ключи NoDispCPL и NoChangingWallpaper:

- ключ *NoDispCPL*: *тип DWORD*, значение параметра «1», расположение – раздел System директории Policies (рис.5.24);
- ключ *NoChangingWallpaper: тип DWORD*, значение параметра «1», расположение – раздел ActiveDesktop директории Policies (рис.5.25):.

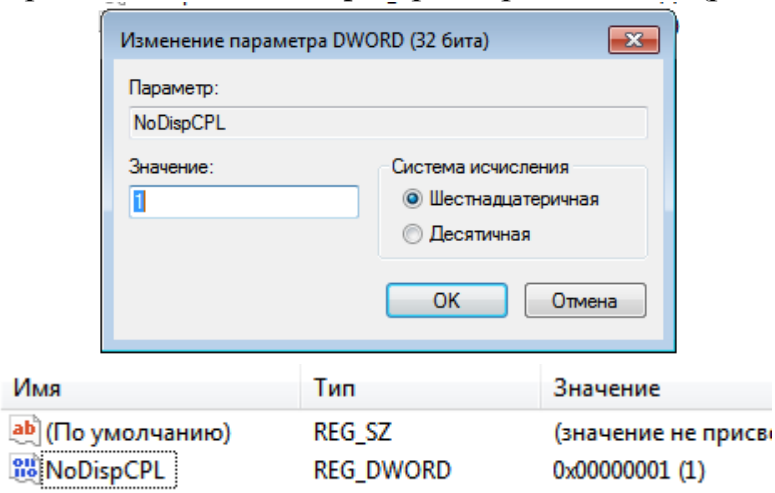


Рис. 5.24. Ключ NoDispCPL раздела System директории Policies

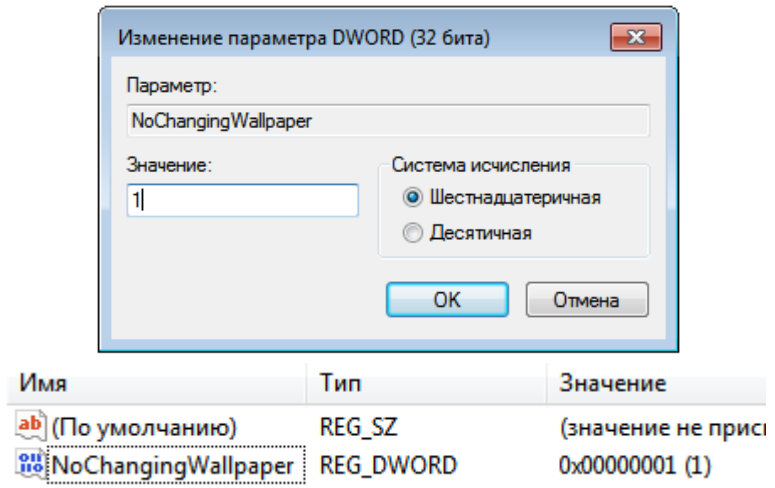


Рис. 5.25. Ключ NoChangingWallpaper раздела ActiveDesktop директории Policies

Проверим применение настроек. Содержимое вкладки «Экран» панели управления до применения изменений (рис.5.26):

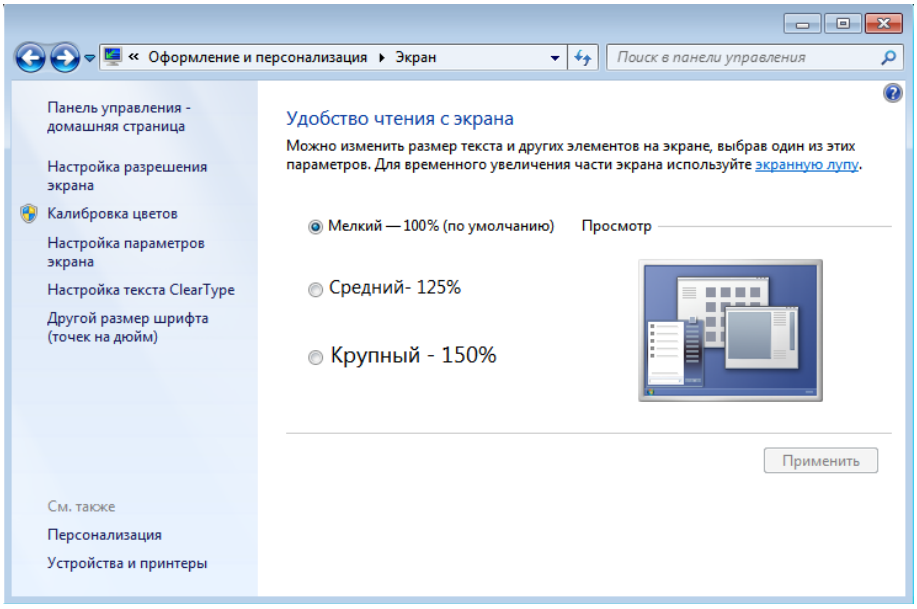


Рис. 5.26. Содержимое вкладки «Экран» панели управления до применения изменений

Содержимое вкладки «Экран» панели управления после применения изменений, то есть после вступления в силу ключа NoDispCPL (рис.5.27):

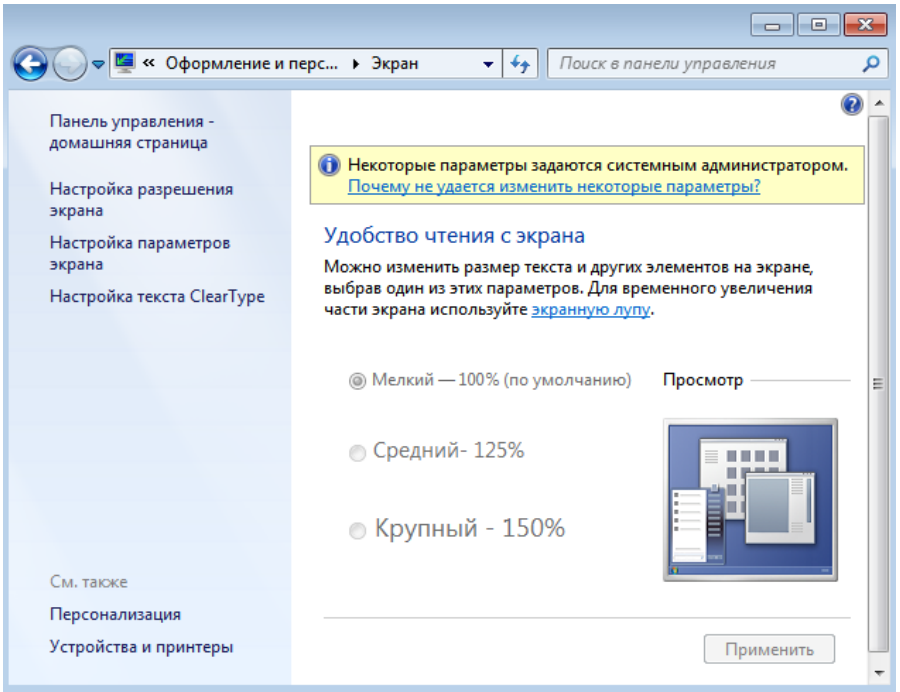


Рис. 5.27. Содержимое вкладки «Экран» панели управления после применения изменений

Изменения очевидны: теперь пользователю недоступно изменение масштабирования экрана, а также появилось предупреждение о том, что

некоторые параметры данной вкладки изменены системным администратором. Соответственно, и отменить данные ограничения также может только системный администратор.

Проверим изменение обоев рабочего стола. Содержимое вкладки «Персонализация» панели управления до применения изменений (5.28):

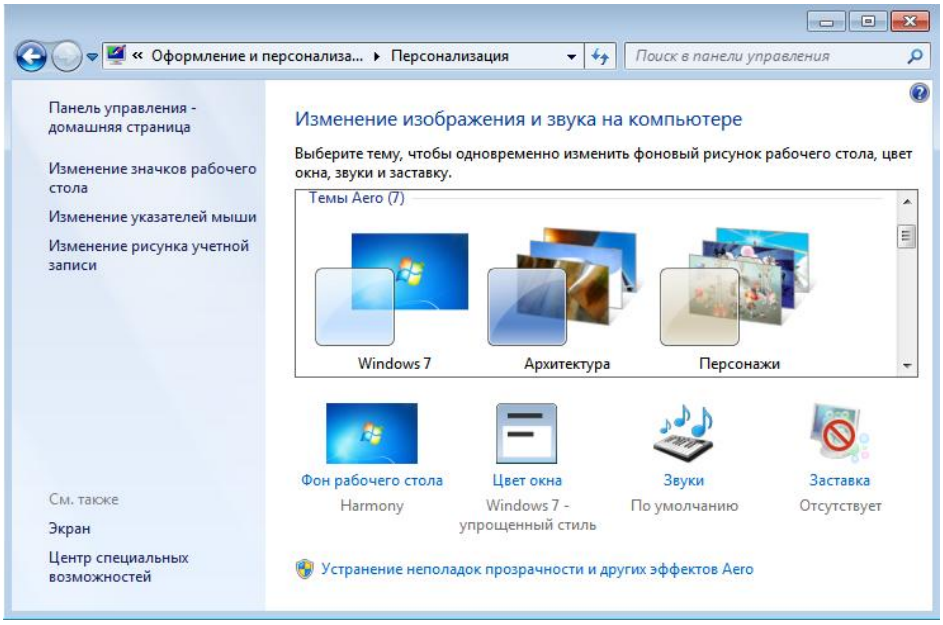


Рис. 5.28. Содержимое вкладки «Персонализация» панели управления до применения изменений

Содержимое вкладки «Экран» панели управления после применения изменений, то есть после вступления в силу ключа NoChangingWallpaper (рис.5.29):

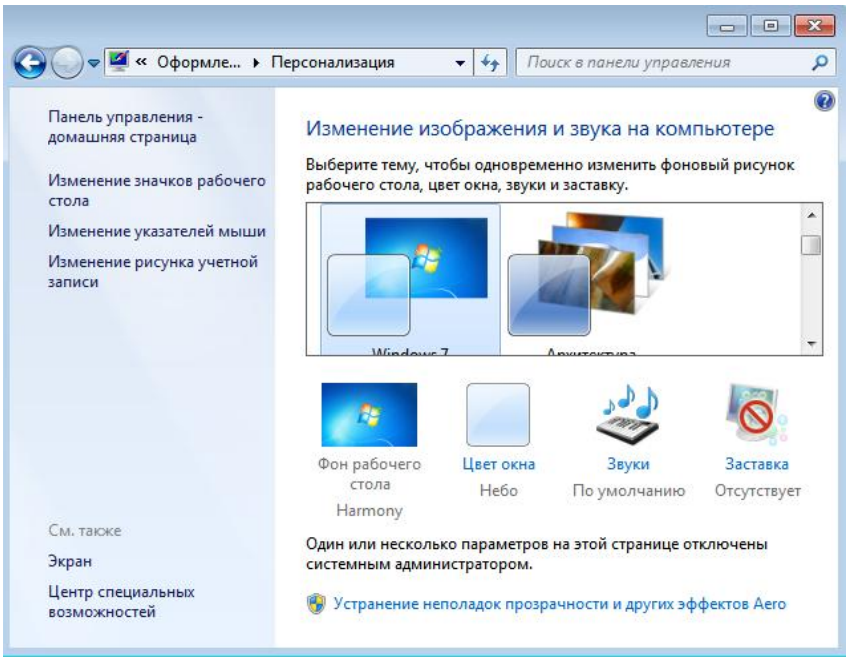


Рис. 5.29. Содержимое вкладки «Персонализация» панели управления после применения изменений

Изменения очевидны: теперь пользователю недоступно изменение фона рабочего стола, соответствующий пункт неактивен, а также появилось предупреждение о том, что некоторые параметры данной вкладки изменены системным администратором. Соответственно, и отменить данные ограничения также может только системный администратор.

Следовательно, ограничение функционала «Панели управления» произведено успешно.

Рассмотрим еще один пример. Отключим возможностьиспользования «Панели управления». Для этого воспользуемся настройкой параметраNoControlPanel (рис.5.30):

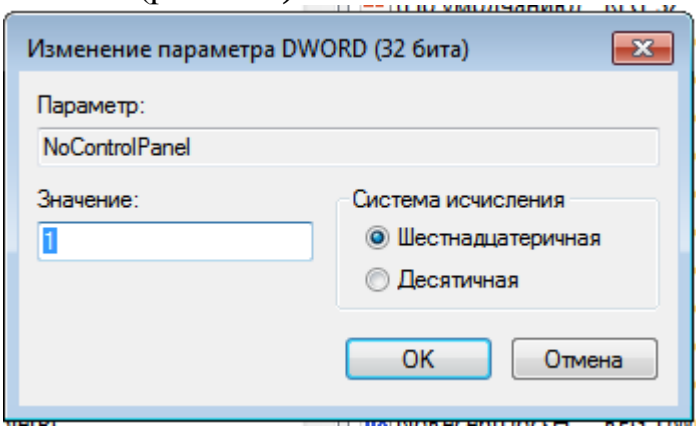


Рис. 5.30. Сортировка значений

Результат применения параметра NoControlPanel(рис. 5.31, 5.32):

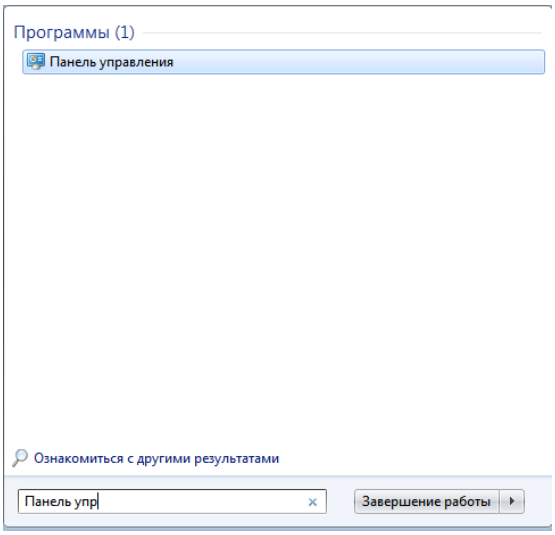


Рис.5.31. Вызов «Панели управления»до применения параметраNoControlPanel

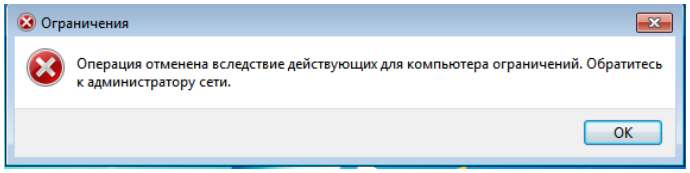


Рис.5.32. Ошибка вызова «Панели управления»после применения параметраNoControlPanel

5.10. ***Отредактировать реестр для закрытия меню кнопки «Пуск» от редактирования***

Закрытие меню кнопки «Пуск» от редактирования используется для того, чтобы зафиксировать доступные для работы пользователя приложения: например, системный администратор в певрый день работы пользователя установит определенный набор программ, доступный для пользователя в соответствии с политикой конфиденциальности предприятия, и зафиксирует его средствами реестра. Для этого следует: в разделе Explorerсоздать аналогично пунктам 5.3 – 5.5 ключ NoChangeStartMenu типа DWORD и настроить значение параметра в «1»(полный путь остался прежним):

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\ Policies(рис.5.33).

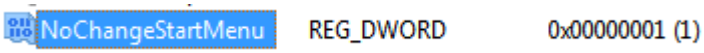


Рис.5.33. КлючNoChangeStartMenuраздела Explorer директории Policies

Функционал меню кнопки «Пуск» до применения изменений (реакция меню кнопки «Пуск» на нажатие ПКМ) показан на рис.5.34:

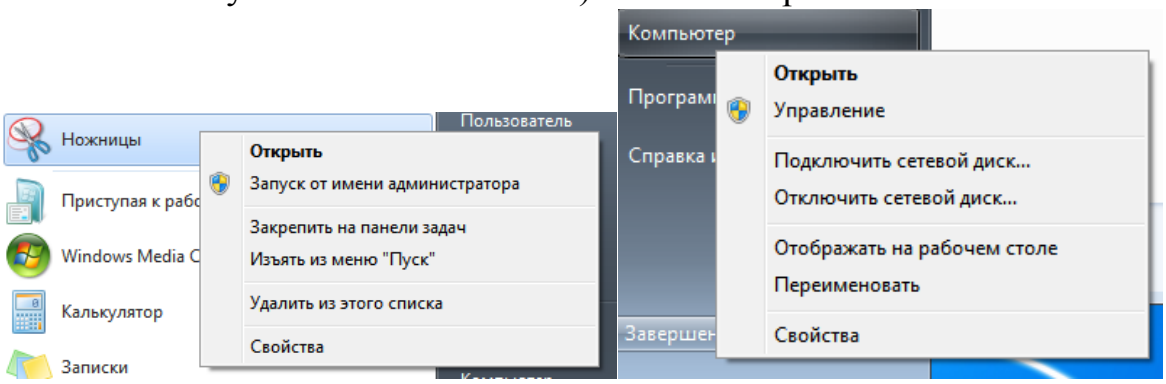


Рис. 5.34. Функционал меню кнопки «Пуск» до применения изменений

После перезагрузки и применения настроек пользователь не сможет вызвать контекстное меню кнопки «Пуск» и, соответственно не сможет редактировать его (рис.5.35).

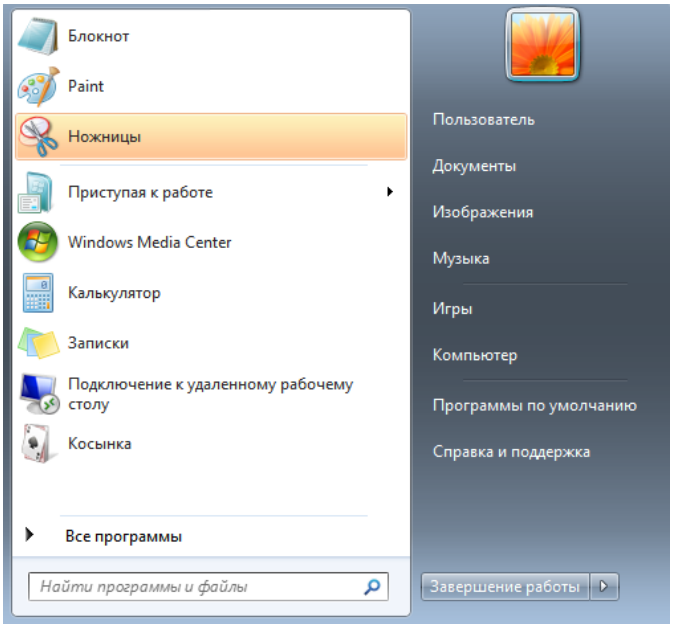


Рис. 5.35. Функционал меню кнопки«Пуск» после применения изменений

Таким образом, ограничение функционала «Панели управления» произведено успешно.

5.11. ***Настроить применение разрешённых USB-накопителей***

USB-устройства плотно вошли в нашу жизнь. В то же время несоблюдение требований политики информационной безопасности по ограничению доступа отчуждаемых носителей к АРМ через внешние порты может привести к серьезным последствиям. Чтобы осуществить настройки применениеконкретного перечня USB-накопителей на АРМ следует выполнить ряд манипуляций с разделами и параметрами реестра. Для начала в окне Редактора реестра нужно найти путь

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR.

Здесь хранится информация обо всех некогда подключенных USB-носителях. Не важно, были ли они удалены, запись о каждомUSB-носителе будет храниться всегда, пока ее не удалить вручную (рис.5.36).

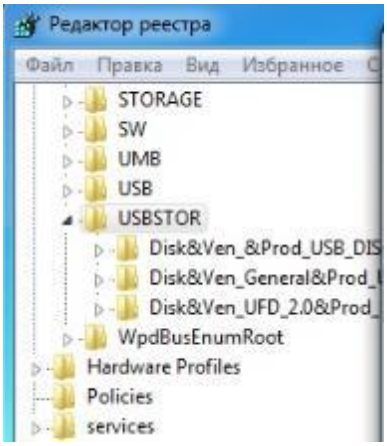


Рис. 5.36 – Содержимое подраздела USBSTOR

Найдя указанный путь в реестре, необходимо очистить все содержимое этой папки. Однако для проведения этой операции требуется получить полный доступ на USBSTOR. Сделать это можно, нажав на папке USBSTOR правой кнопкой мыши (ПКМ), и выбрать Разрешения. В открывшемся окне следует выделить группу Все, которой дать Полный доступ (рис. 5.37).

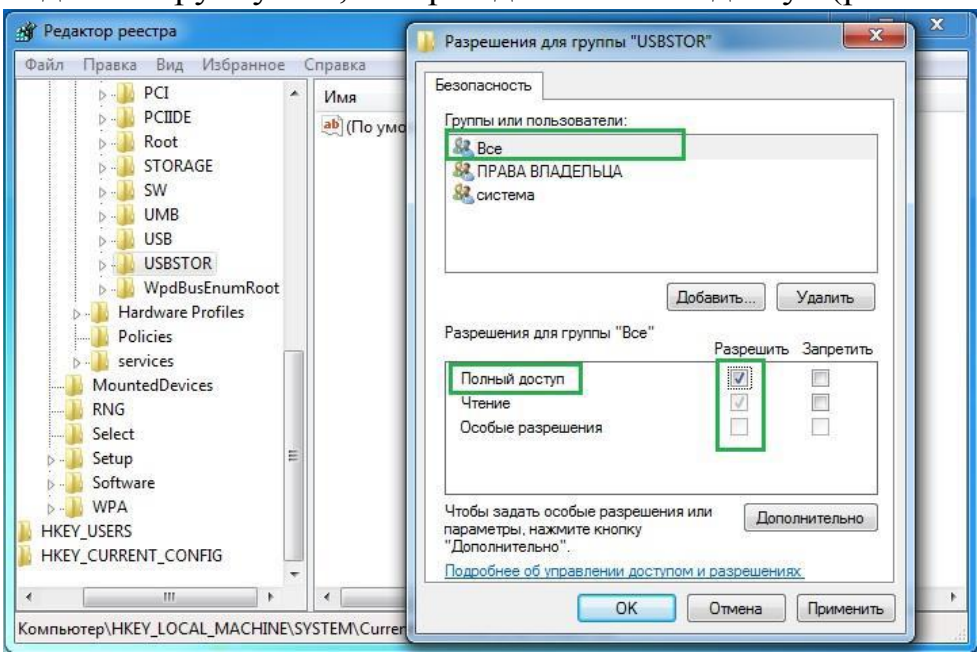


Рис. 5.37 – Получение разрешений

Теперь, когда полный доступ к папке USBSTOR открыт, можно удалить все, что в ней находится (рис. 5.37).

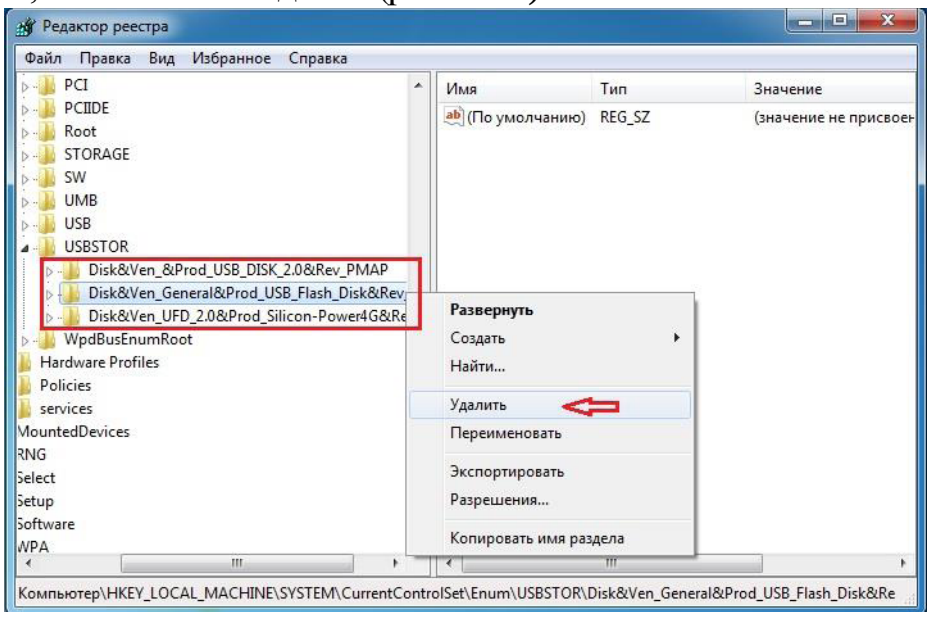


Рис. 5.37.Удаление содержимого подраздела

Следующим шагом нужно открыть доступ USB-носителю, который будет использоваться на нашем АРМ. Для этого следует вставить USB-носитель в разъем USB и подождать, пока она полностью установится. После того, как USB-носитель определился, клавишей F5 требуется обновить окно

реестра. В папке USBSTOR появится дополнительная папка — это и есть информация о новомUSB-носителе, например,

Disk&Ven_Verbatim&Prod_STORE_N_GO&Rev_5.00.

Теперь, когда нужныйUSB-носительзанесен в реестр, нужно вернуться к папке USBSTOR и снова поменять права - у группы Все (снять флажок Полный доступ). Пункт Чтение оставить (рис. 5.38).

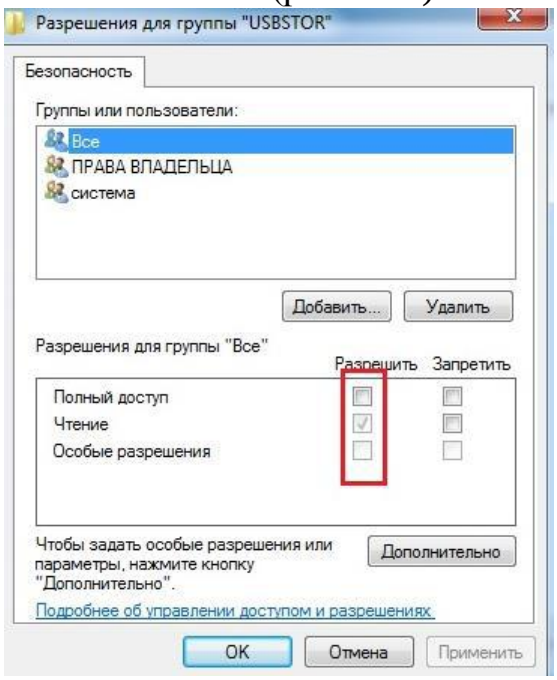


Рис. 5.38. Повторное изменения прав – ограничение прав

После этого такие же права необходимо назначить группе Система (SYSTEM). Для этого, все в этом же окне Разрешения, нужно выбрать группу Система и ниже нажать кнопку Дополнительно (рис. 5.39).

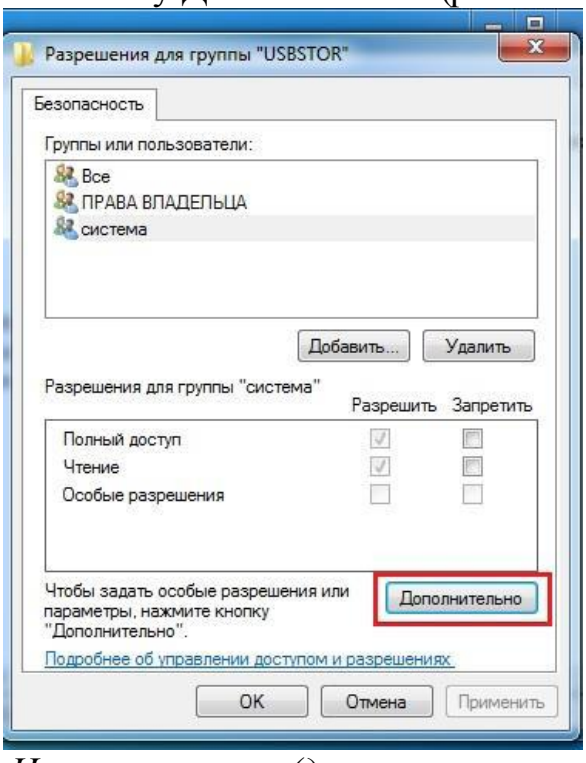


Рис. 5.39 – Назначение прав (дополнительные настройки)

После этого откроется окно Дополнительные параметры безопасности для USBSTOR, в котором следует убрать метку Добавить разрешения, наследуемые от родительских объектов, а во всплывшем окне нажать Добавить (рис. 5.40).

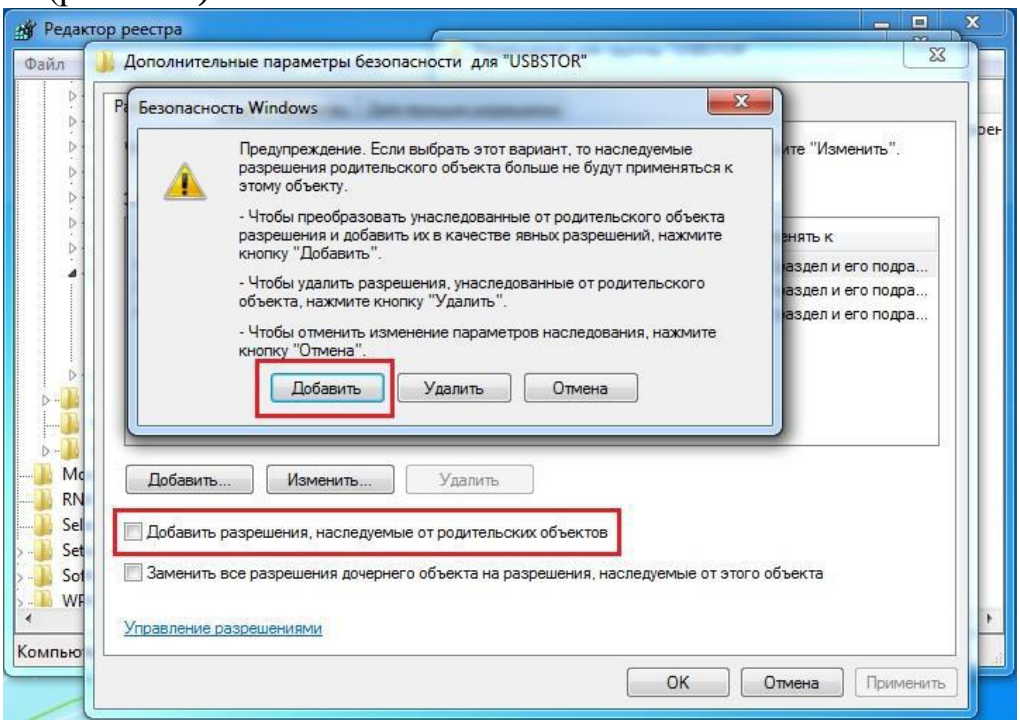


Рис.5.40.Настройка окнадополнительные параметры безопасности для USBSTOR

Теперь, права пользователя Система доступны для изменений. Аналогично, как и с группой Все, нужно убрать у группы Система Полный доступ, при этом пункт Чтение оставить без изменений. Последним шагом следует нажать кнопку Дополнительно (группа Система), в открывшемся окне включитьопцию «Заменить все разрешения дочернего объекта на разрешения, наследуемые от этого объекта» (рис. 5.41).

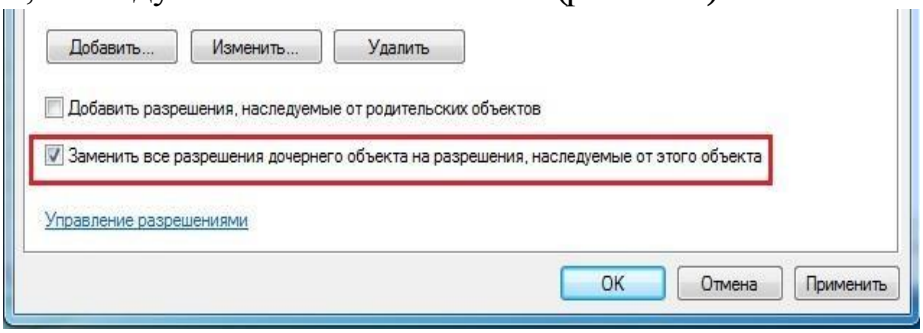


Рис. 5.41. Замена разрешений дочернего объекта

Таким образом, после всех произведенных настроек, теперь на АРМ работает только одинразрешенный USB-носитель, который был прописан. Можно прописать разрешения на применение несколько USB-носителей. Остальные же, система будет определять, но работу с ними блокировать (рис. 5.42).

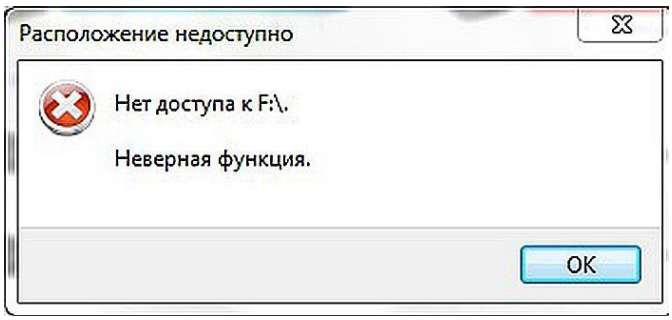


Рис. 5.42. Ошибка при попытке работать с заблокированным USB-носителем

Выводы по лабораторной работе

В лабораторной работе была изучена и настроена изолированная программная среда на АРМ «закрытого» контура ИС средствами ОС Windows 7 с целью защиты АРМ от НСД. В ходе данной лабораторной работы было изучено следующее:

- как вызывать реестр для настройки безопасности сети;
- как добавлять параметры в разделы реестра;
- как устанавливать значения для конкретных параметров реестра;
- как экспортировать настройки реестра для последующего упрощения конфигурации.

В частности, были осуществлены следующие настройки:

- Редактирование ключей реестра раздела Explorer для ограничения функционала рабочего стола и меню «Пуск» пользователя;
- Редактирование реестра для ограничения функционала «Панели управления» пользователя;
- Редактирование реестра для ограничения функционала меню «Пуск» пользователя.

Использование параметров редактора реестра существенно способствует увеличению безопасности системы, поскольку работа с редактором доступна только системному администратору.

Проведенные настройки реестразначительно ограничивают работу пользователя в системе. С точки зрения защиты от НСД к АРМ усложняется работа злоумышленника при успешном внедрении в систему. Например, злоумышленник лишен возможности просмотреть недавно открытые файлы пользователя, а также воспользоваться возможностями пункта меню «Выполнить» кнопки «Пуск» для открытия нужных ресурсов и так далее. После настройки ИПС ни пользователь, ни злоумышленник не смогут получить доступ к закрытым данным и/или повлиять на работу системы в целом.Изолированная программная среда существенно повышает защищенность системы от программных закладок, т.к. вредоносное ПО чаще всего нарушает работу ОС путем редактирования реестра.

В то же время ИПС создает определенные сложности в администрировании защищаемой системы. Неправильная настройка параметров может привести к некорректной работе операционной системы. Например, при установке нового программного продукта администратор обязан модифицировать списки разрешенных программ для пользователей, с учетом того, что они должны иметь возможность работать с этим программным продуктом.

6. Содержание отчета

6.1. Цель работы
6.2. Теоретические сведения
6.3. Последовательность выполнения лабораторной работы
6.4. Возможности реестра ОСWindows, в которой выполняется работа
6.5. Обоснование настроек каждого ключа реестра раздела Explorer для ограничения функционала рабочего стола и меню «Пуск» пользователя
6.6. Редактирование реестра для ограничения функционала «Панели управления».
6.7. Редактирование реестра для закрытия меню «Пуск».
6.8. Вывод о значимости замкнутой программной среды и ее настройки для защиты АРМ от НСД.

7. Контрольные вопросы

7.1. Для чего создается изолированная программная среда на АРМ пользователя?
7.2. Как осуществляется организация ИПСсредствами ОС Windows?
7.3. Что представляет собой редактор реестра в ОС Windows?
7.4. Что содержатсписки главных разделов (rootkeys) редактора реестра в ОС Windows?
7.5. Как строится структура реестра ОС Windows?
7.6. Какие виды параметров (ключей) реестра вы знаете?
7.7. За что отвечает РазделExplorer?
7.8. Через свойства какого разделапроизводитсясоздание раздела Explorer?
7.9. Для чего производят экспорт директории Explorer?
7.10. Как вносятся изменения в реестр чтобы в результате была установлена ИПС?
7.11. Как проводится редактирование реестра для ограничения функционала «Панели управления»?
7.12. Как проводится редактирование реестра для закрытия меню «Пуск»?

Библиографический список

1. ГОСТ Р ИСО 7498-2–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть.2. Архитектура защиты. М.: ИПК «Издательство стандартов», 1999.
2. Мошак Н.Н., Тимофеев Е.А. Особенности построения политики информационной безопасности в инфокоммуникационной сети // Электросвязь. 2005, №9.
3. Мошак Н. Н. Защищенные инфотелекоммуникации. Анализ и синтез: монография. СПб.: ГУАП, 2014. 193 с.
4. Мошак Н.Н., Татарникова Т.М. Защита сетей от несанкционированного доступа. Учеб. пособие / СПб.: ГУАП, 2014. с. 121.
5. Зима В., Молдовян А., Молдовян.Н. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2000. 320 с.
6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника. 2004.
7. Мошак Н.Н. Безопасность информационных систем: Учеб. пособие/ Н.Н.Мошак – СПб.: ГУАП, 2019. – 169 с.
ISBN 978-5-8088-1414-1