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. Теоретические положения

Существует «закрытый» и «открытый» контуры обработки, хранения и передачи информации. В «закрытом» контуре обрабатывается конфиденциальная информация с различным грифом секретности. В «открытом» контуре – открытая информация.

Подсистема защиты АРМ от НСД «закрытого» и «открытого» контура должна обеспечивать:

- однозначную идентификацию пользователей в ИС и в операционной системе АРМ (использование общих идентификаторов не допускается;
- идентификацию по логическим именам информационных ресурсов (логических устройств, каталогов, файлов).
- 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.

Управление доступом в АРМ должна базироваться на стандартных механизмах идентификации, аутентификации и разграничения доступа предоставляемых: BIOS ПЭВМ; сертифицированным программно-аппаратным комплексом защиты от НСД СЗИ; ОС Windows АРМ; сетевой ОС; СУБД; средствами усиленной аутентификации ACE Server (SecurID) или Kerberos.

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.

3. Процесс выполнения работы.

3.1. Подготовка к настройке локальных политик безопасности.

Установка макета варианта лабораторной работы на диске С.

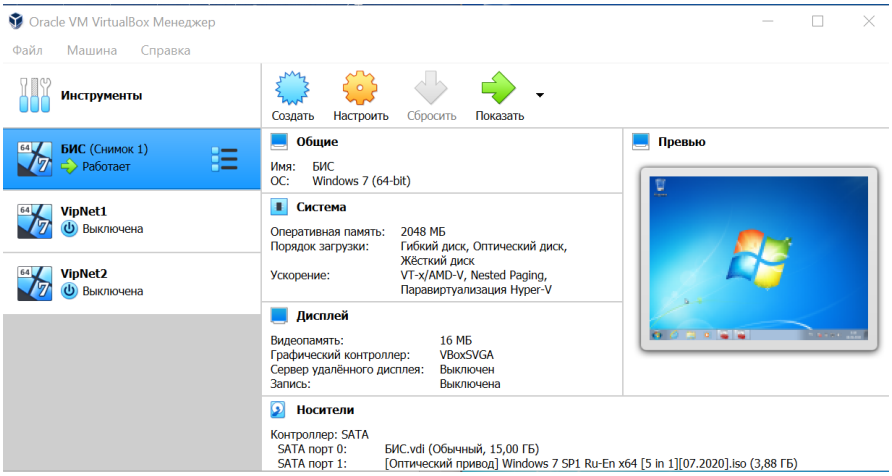

Рисунок 1 - Подготовка виртуальной машины

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»*

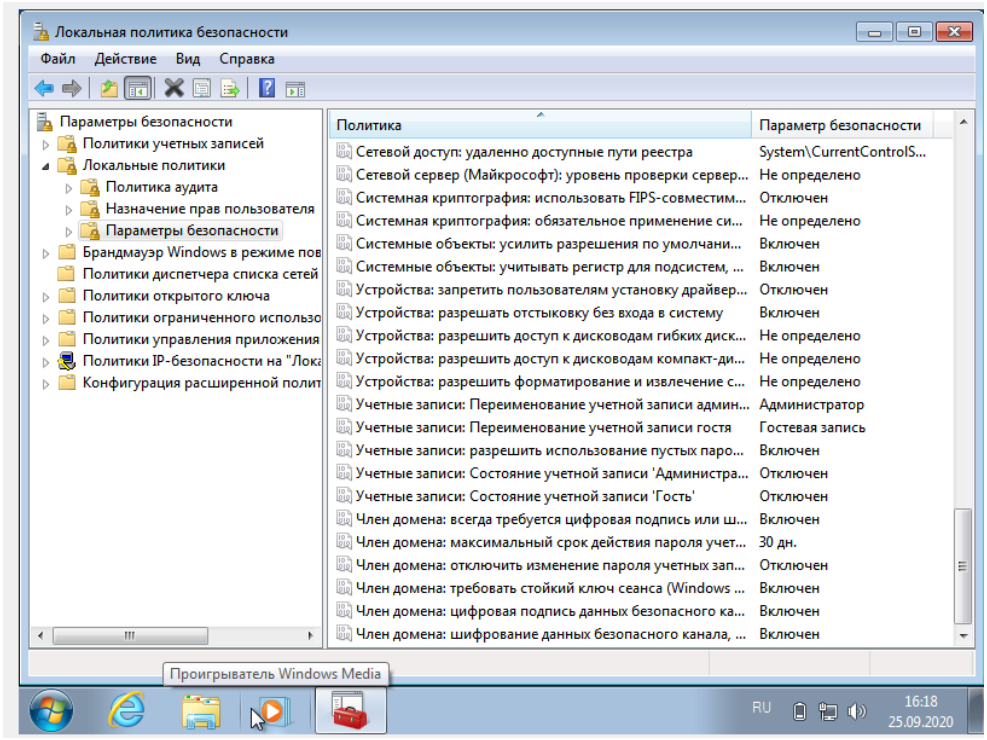

Рисунок 2 - Открытие локальной политики безопасности

3.2. Управление встроенными учетными записями

Необходимо переименовать гостевую учетную запись. Для этого выполняются следующие действия:

a) Открыть оснастку *«Локальные политики безопасности»*

b) Перейти в узел «Локальные политики», а затем «Параметры безопасности»

c) Открыть параметр «Учетные записи: Переименование учетной записи гостя»

d) В текстовом поле ввести *Гостевая запись* и нажать на кнопку «ОК»

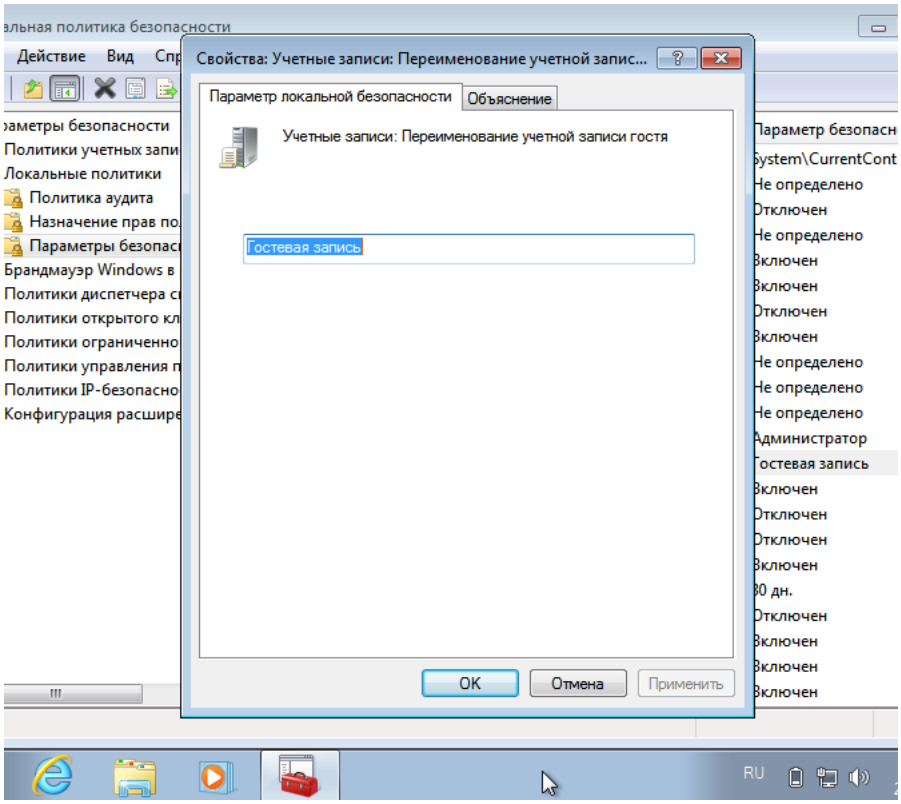

Рисунок 3 - Новое имя пользователя

e) Перезагрузите компьютер.

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

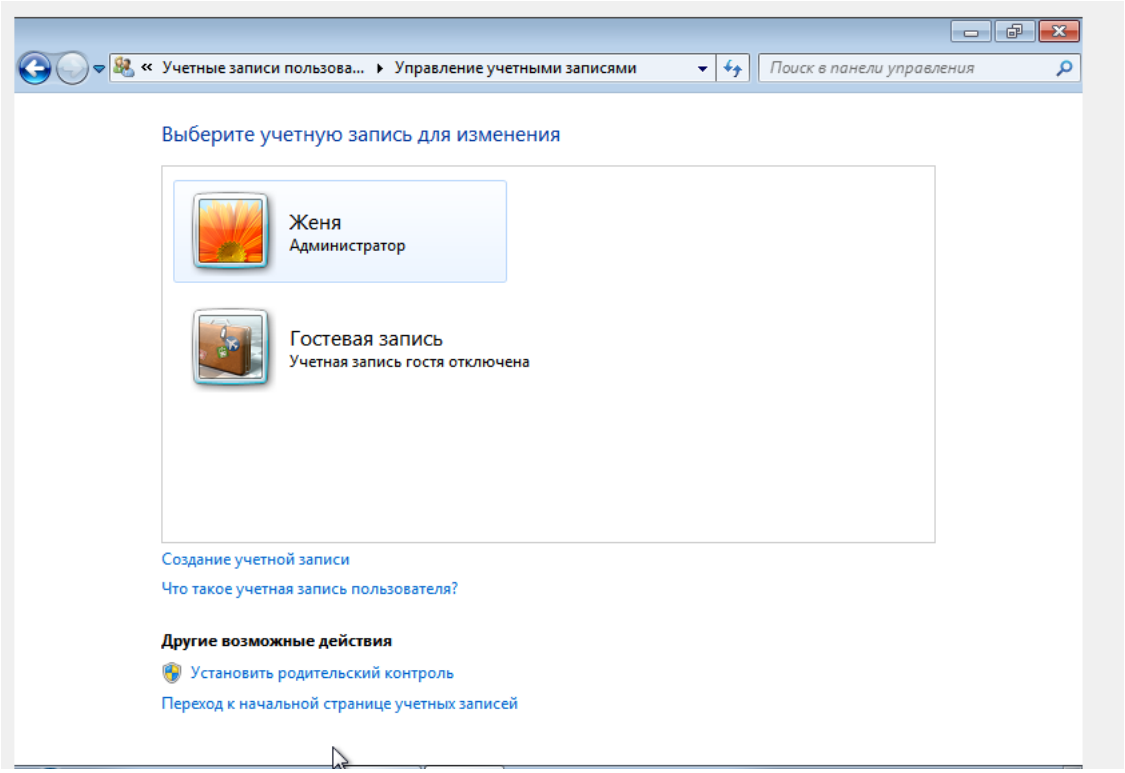

Рисунок 4 - Корректно измененное имя пользователя

3.3. Управление политиками паролей

a) Открыть оснастку «Локальные политики безопасности»;

b) Перейти в узел «Политики учетных записей» и открыть параметр «Политики паролей».

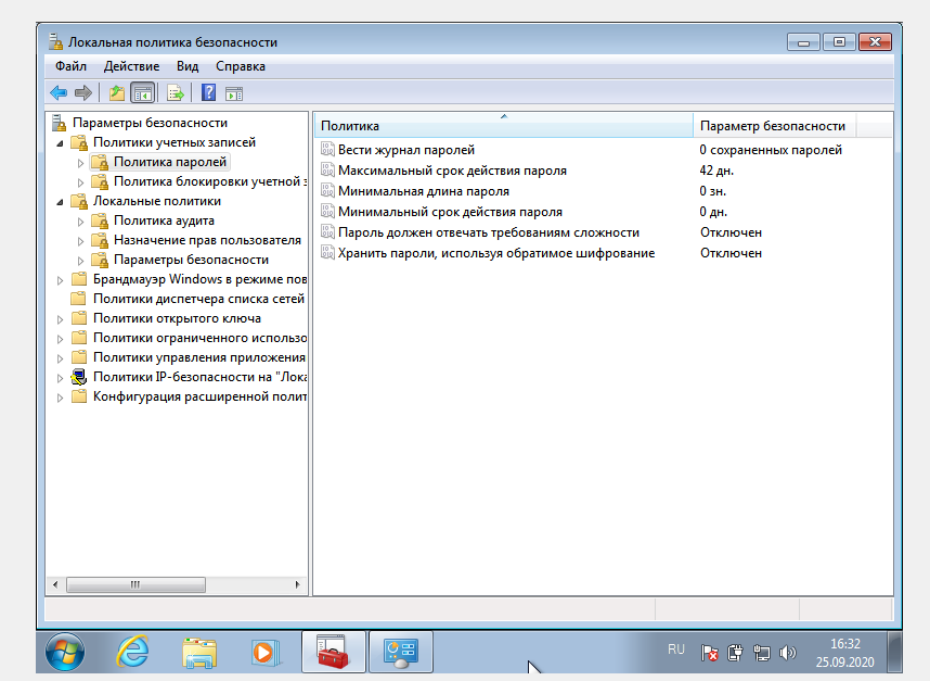

Рисунок 5 – Параметр «Политика паролей»

Т.к. в требованиях к типу ИС 1Б указано, что «должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;», то минимальная длина пароля установлена на восемь символов, также отмечен пункт о необходимости соблюдения требований сложности и хранения паролей, не используя обратное шифрование, т.к. это повышает общую безопасность системы.

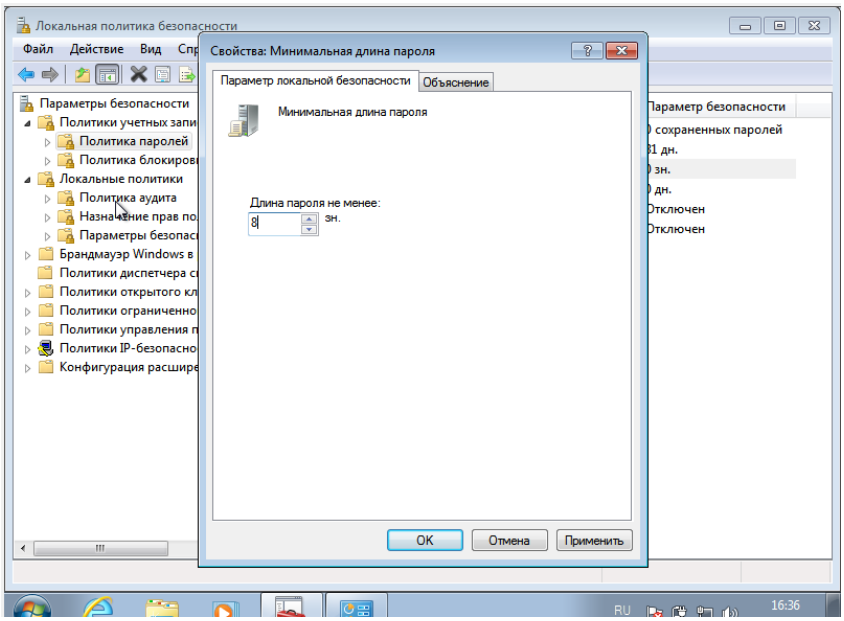

Рисунок 6 – Изменение политики безопасности пароля

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.

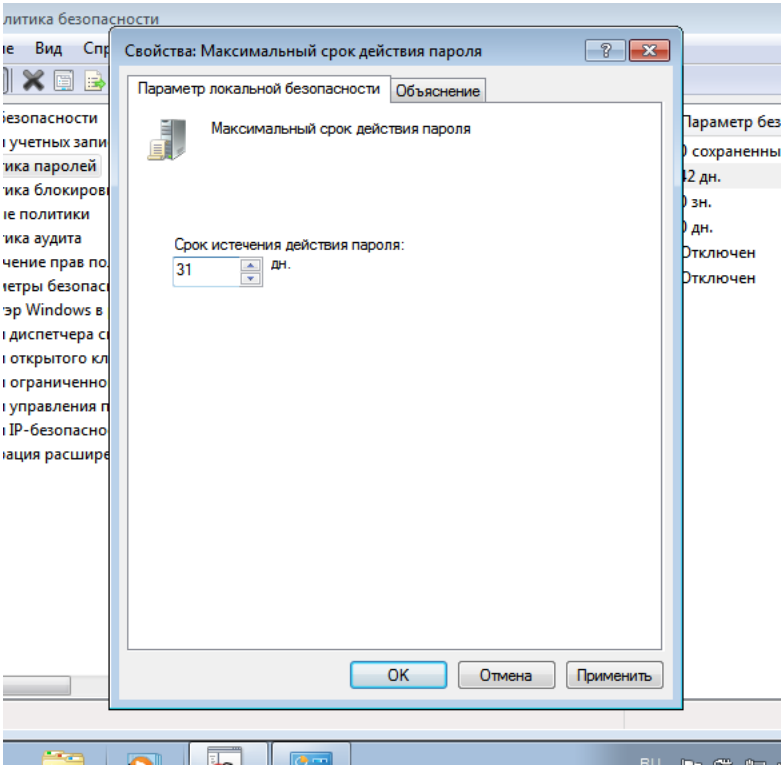

Рисунок 7 - Изменение политики безопасности пароля

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.

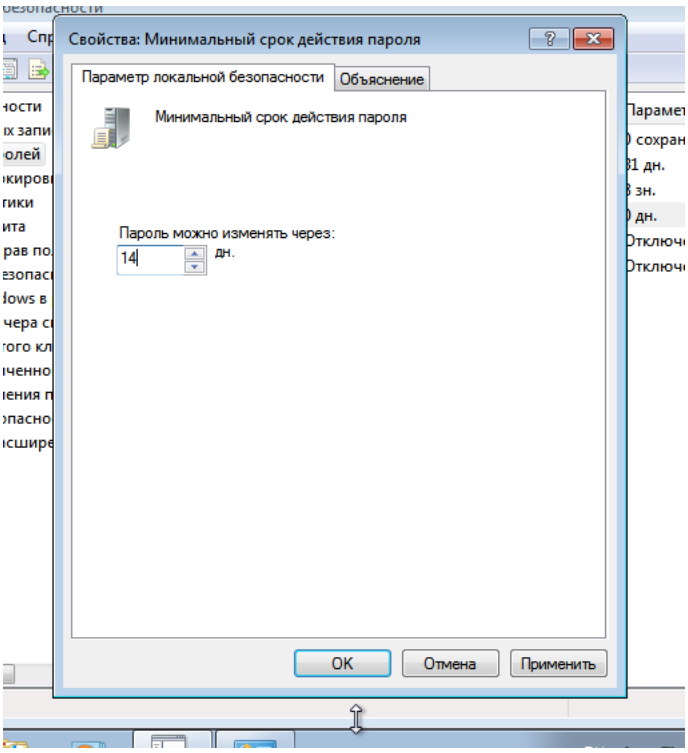

Рисунок 8 - Изменение политики безопасности пароля

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;
- не содержать имени учётной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

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 следующий параметр.

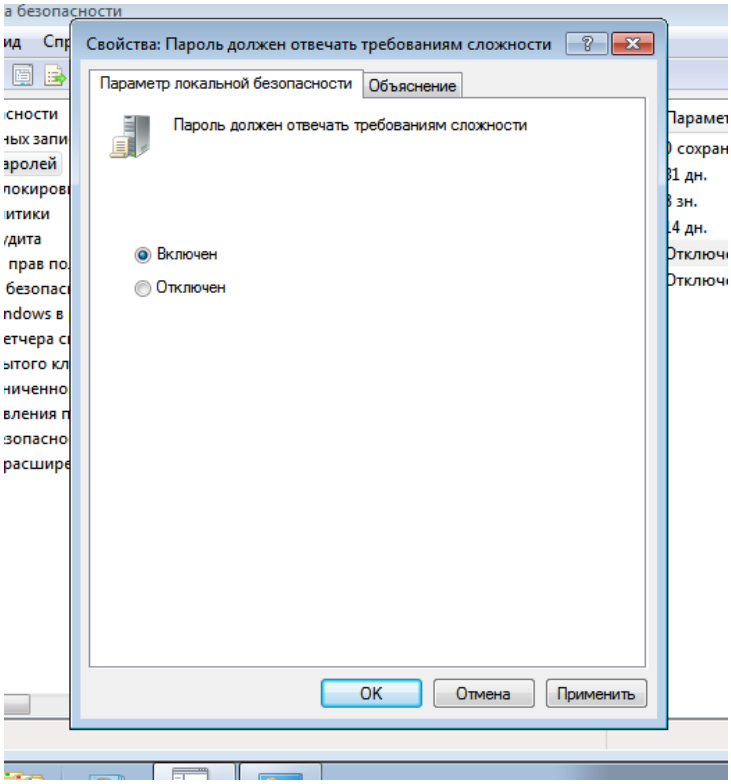

Рисунок 9 - Изменение политики безопасности пароля

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 следующий параметр на значение 5. Таким образом, пользователю необходимо будет придумать как минимум 6 новых паролей.

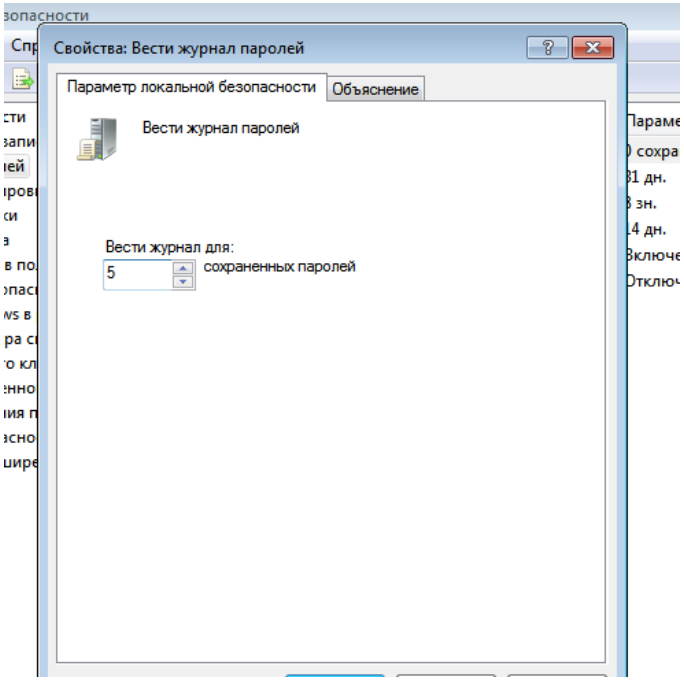

Рисунок 10 - Изменение политики безопасности пароля

Включать обратимое шифрование не стоит, поскольку включение данной политики значительно понизит безопасность паролей.

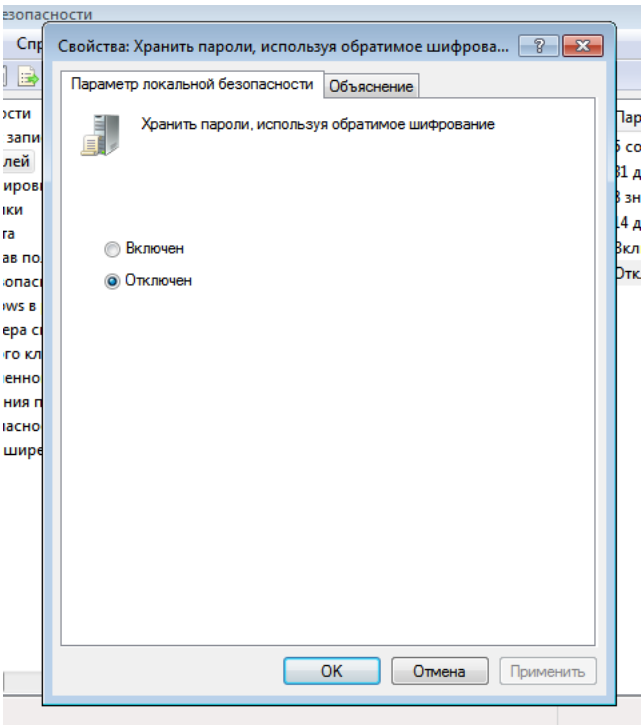

Рисунок 11 - Изменение политики безопасности пароля

3.4. Политика блокировки учетной записи

а) Открыть оснастку *«Локальные политики безопасности»*;

b) Перейти в узел «Политики учетных записей» и открыть параметр «Политика блокировки учетных записей».

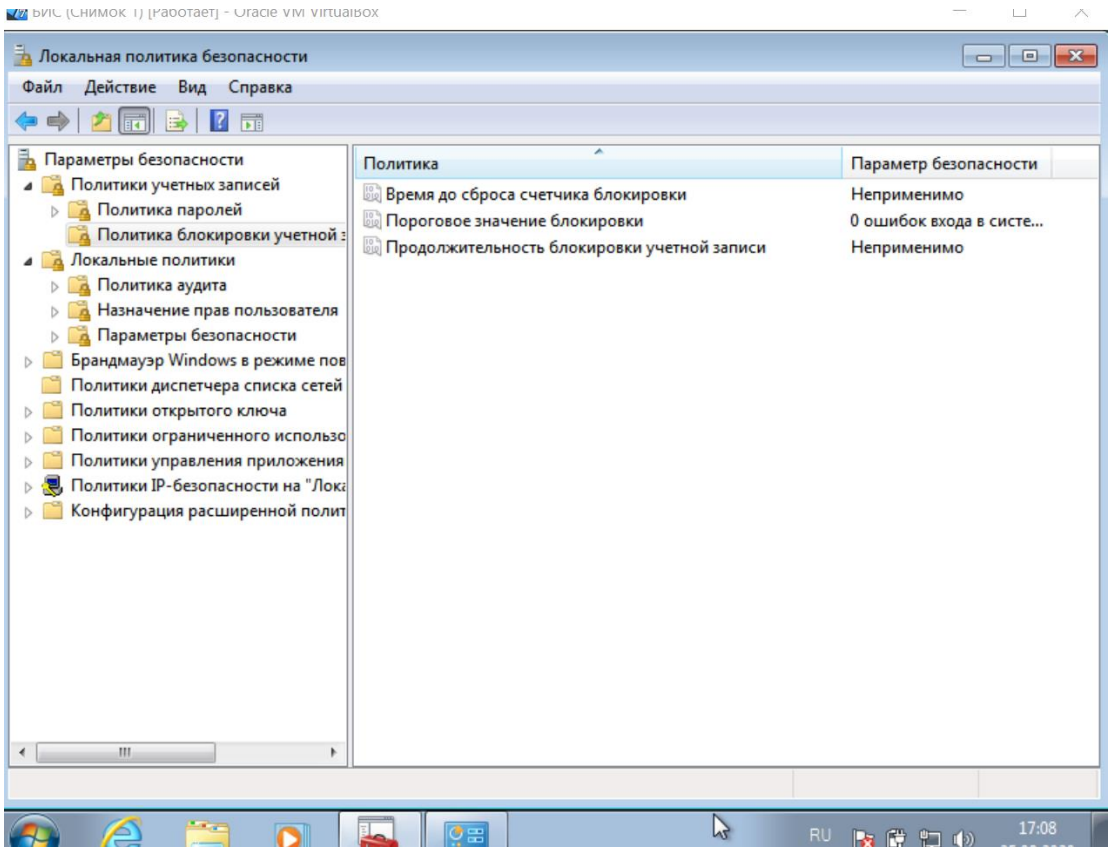

Рисунок 12 - «Политика блокировки учетных записей».

Количество неудачных попыток входа может варьироваться от 0 до 999. Оптимальное количество от трех до семи попыток. При помощи установки продолжительность блокировки учетной записи можно указать время, в течение которого учетная запись будет заблокирована до ее автоматической разблокировки. При помощи политики «Установка время до сброса счетчиков блокировки» устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Это значение должно быть меньше значения политики *«Продолжительность блокировки учетной записи»*.

Зададим пороговое значение «5», таким образом, если пользователи введут 5 раз неверный пароль, учетная запись будет заблокирована.

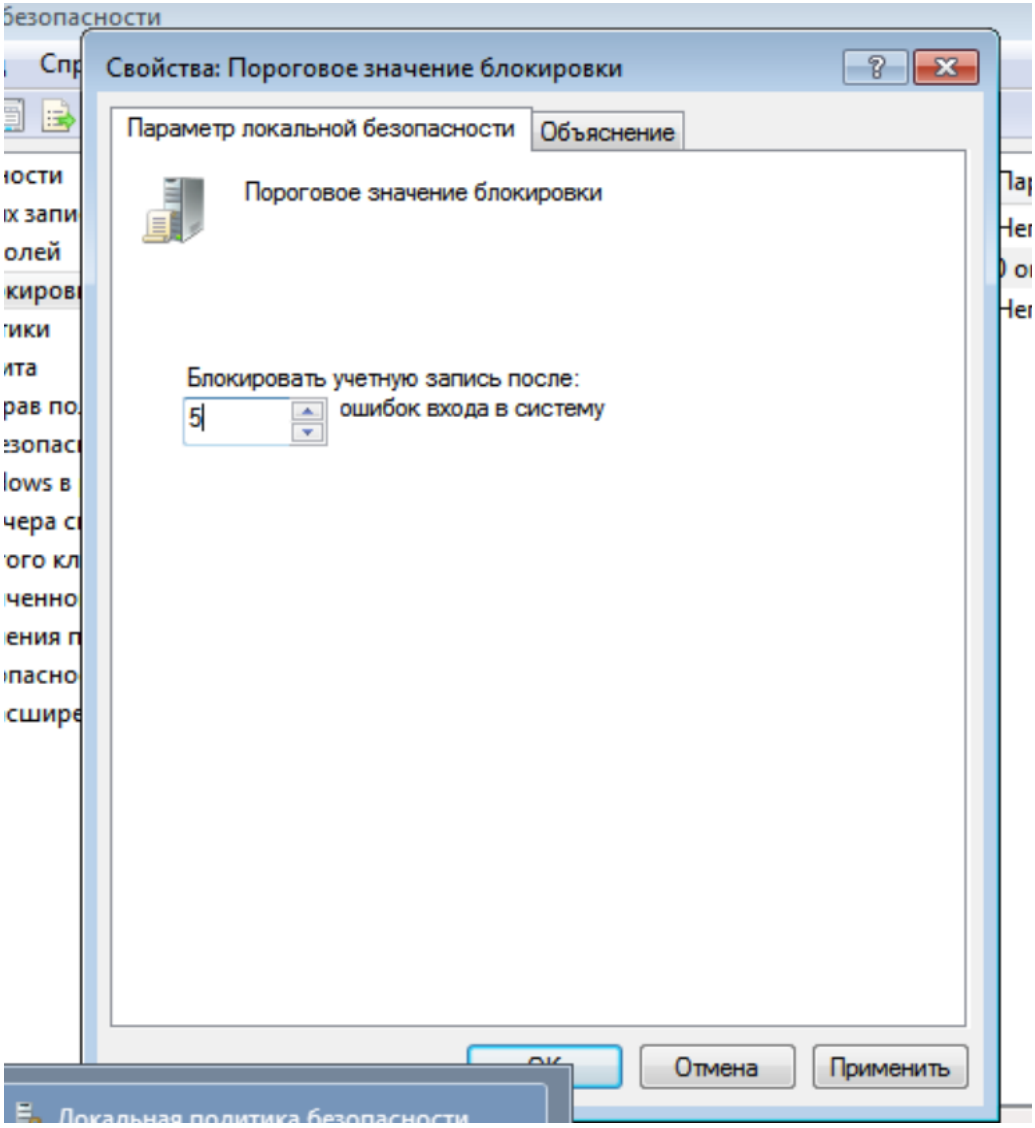

Рисунок 13 – Изменение политики блокировки учетных записей.

Нет необходимости в большом времени до сброса счётчиков блокировки, поэтому значение следующего параметра в 60 минут будет вполне удовлетворительным.

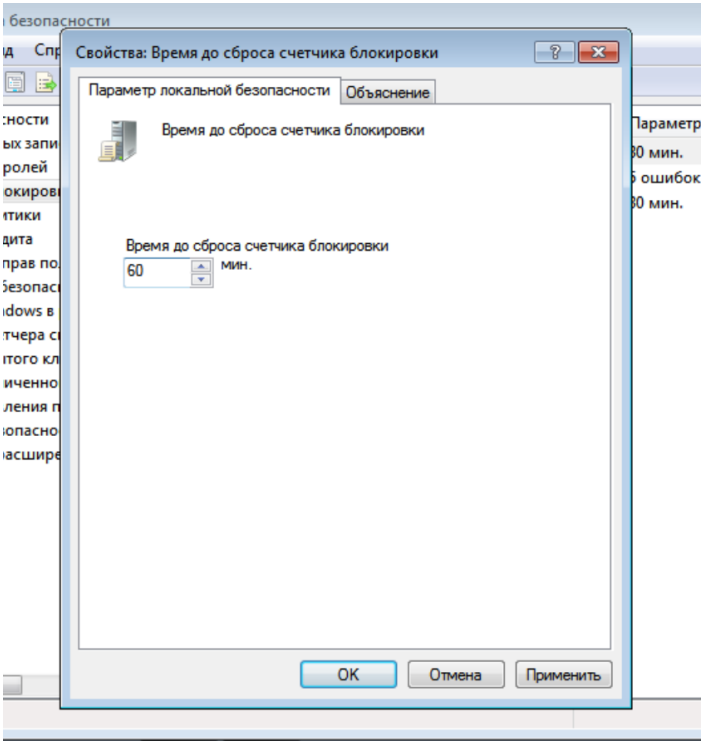

Рисунок 14 – Изменение политики блокировки учетных записей.

Нет необходимости в большом времени блокировки учетной записи, поэтому значение параметра в 60 минут будет вполне удовлетворительным.

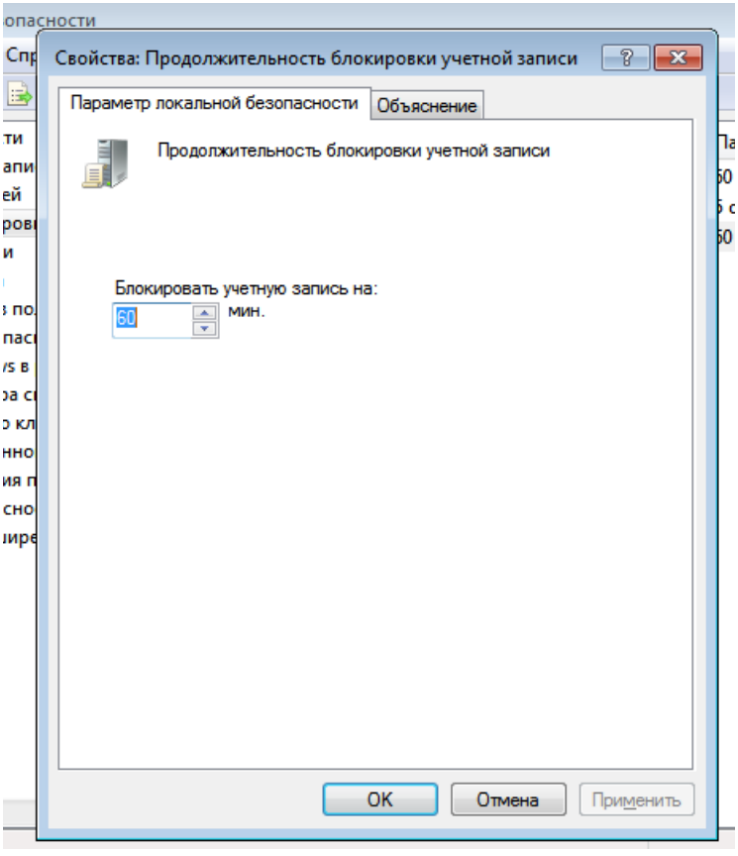

Рисунок 15 – Изменение политики блокировки учетных записей.

3.5. Политика аудита

a) Открыть оснастку *«Локальные политики безопасности»;*

b) Перейти в узел «Локальные политики» и открыть параметр «Политика аудита».

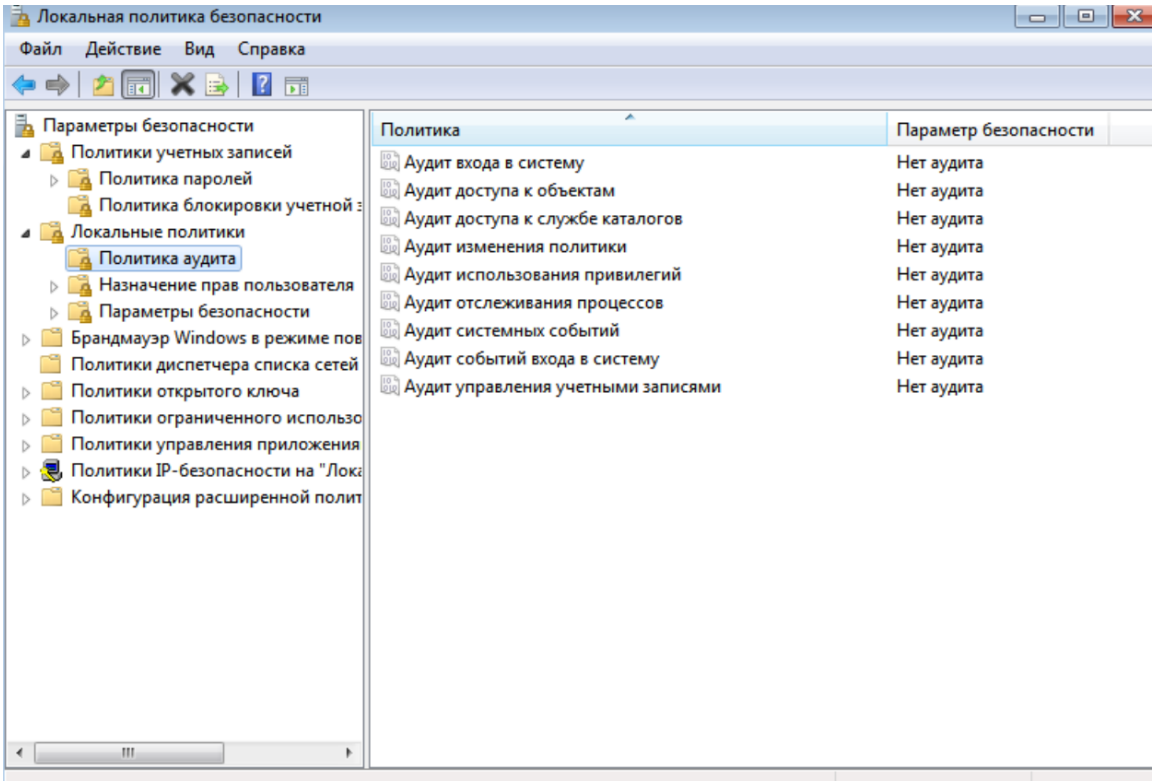

Рисунок 16 - Политика аудита

В требованиях к типу безопасности 1Б указано, что «должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС». Следовательно, необходимо настроить аудит входа в систему и аудита событий входа в систему.

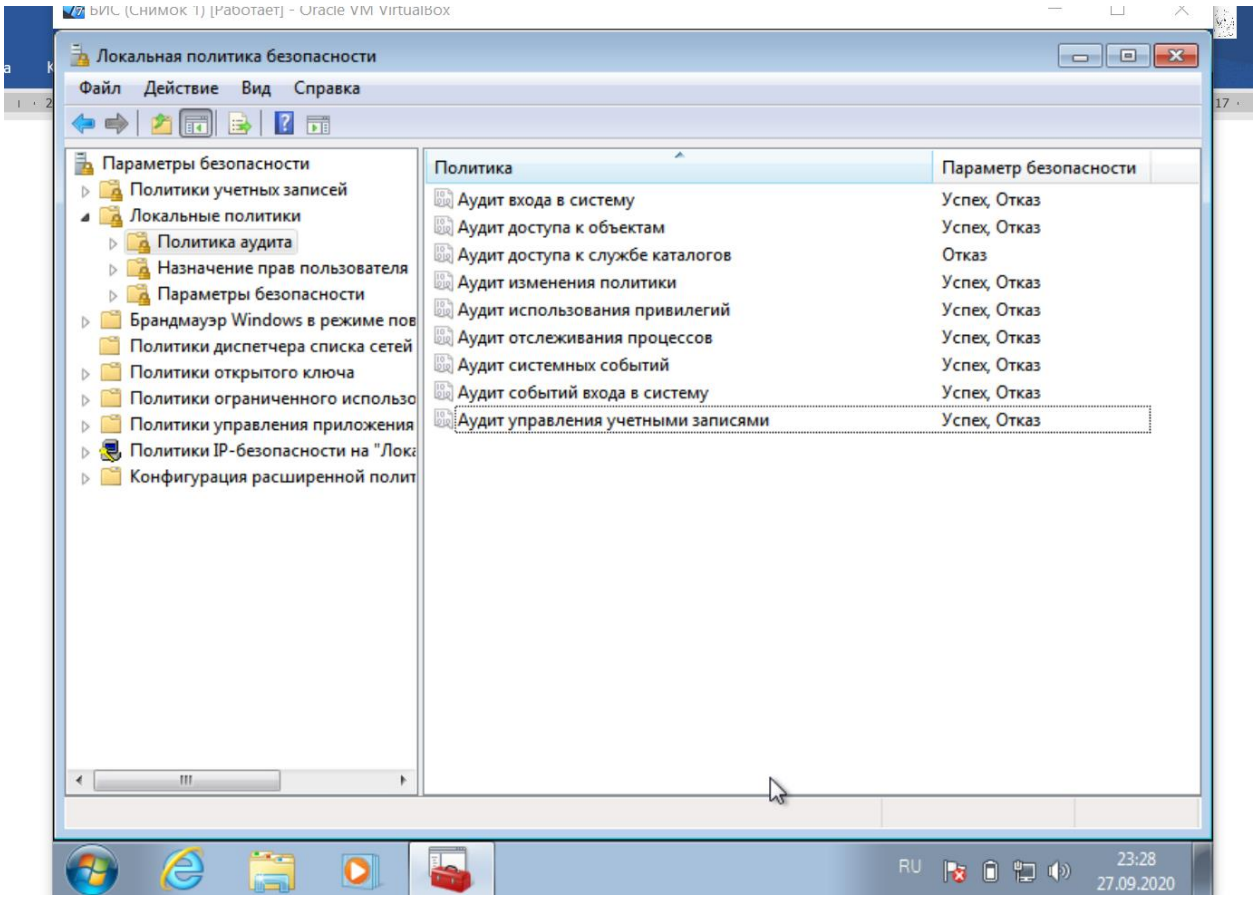

Рисунок 17 - Изменённая политика аудита

3.6. Политика назначения прав пользователей

a) Открыть оснастку *«Локальные политики безопасности»*;

b) Перейти в узел «Локальные политики» и открыть параметр «Назначение прав пользователя».

Изменение системного времени.

Эта политика отвечает за изменение системного времени. Было решено оставить эту привилегию только администраторам.

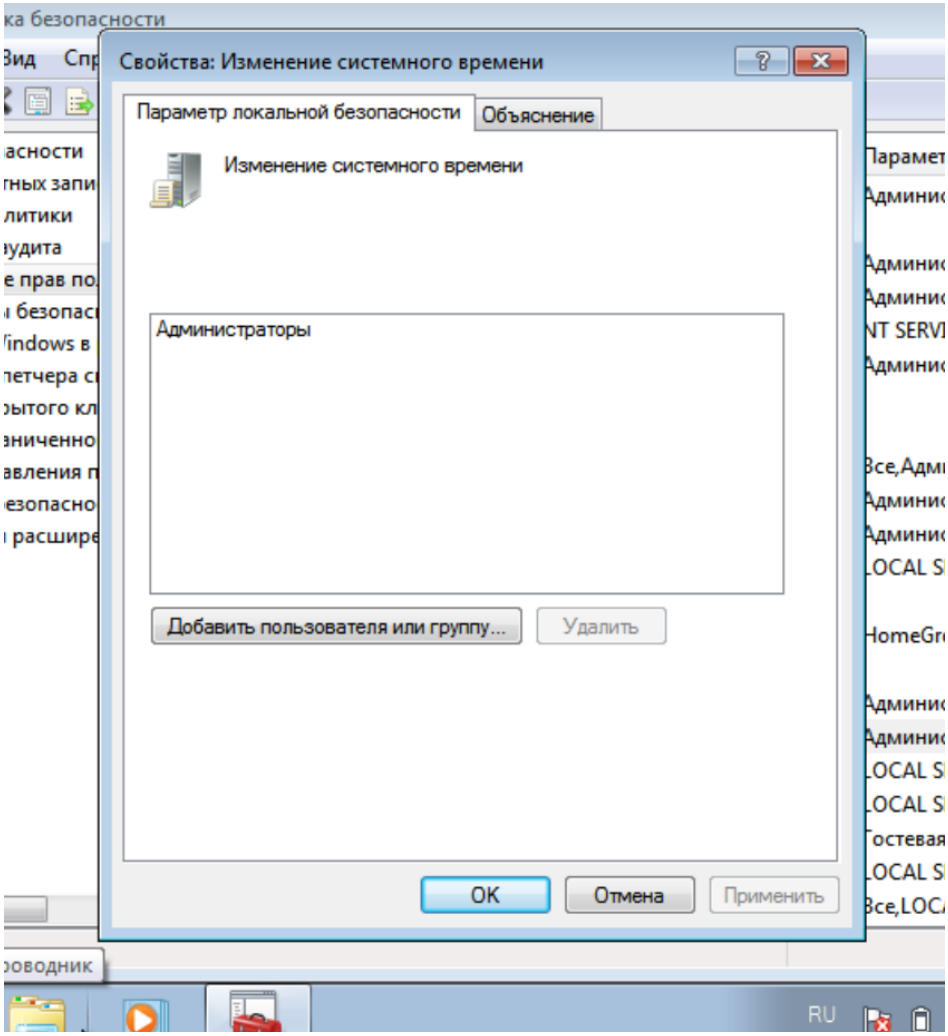

Рисунок 18 - Изменённой параметр «Изменение системного времени»

Завершение работы системы.

Используя этот параметр политики, можно составить список пользователей, которые имеют право на использование команды «Завершение работы» после удачного входа в систему.

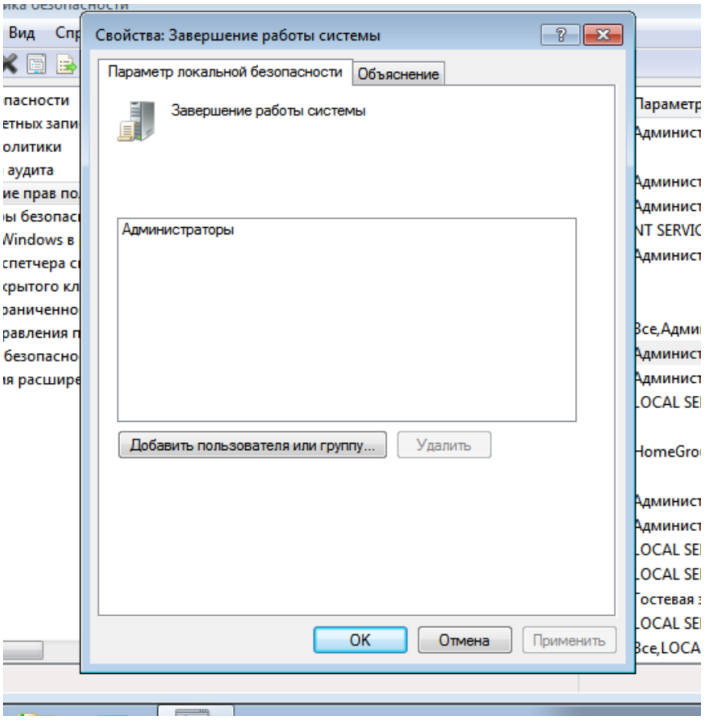

Рисунок 19 - Изменённой параметр «Завершение работы системы.»

Разрешить вход в систему через службу удаленных рабочих столов.

При помощи данной политики безопасности можно ограничить пользователей. Оставляем эту функцию только администратору.

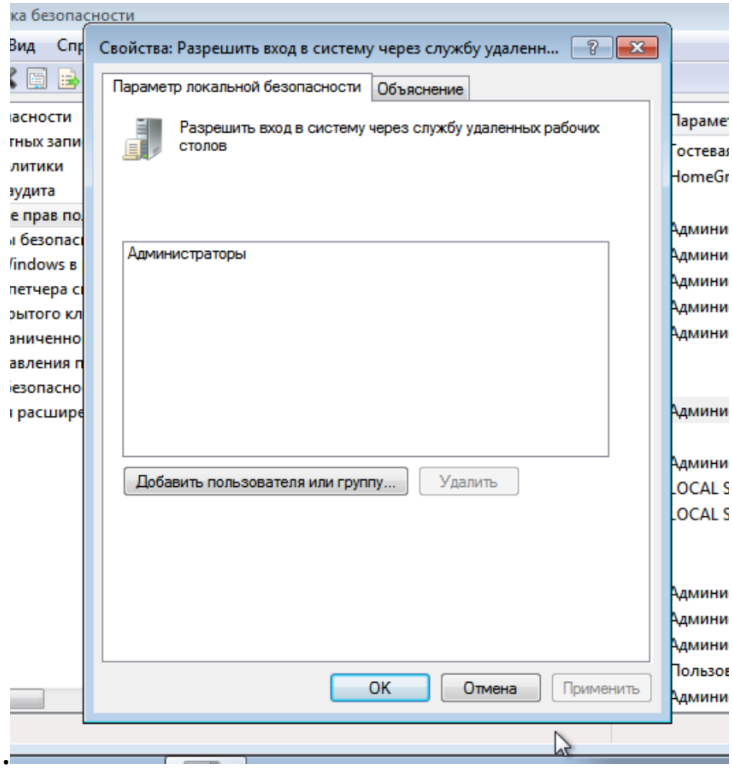

Рисунок 20 - Изменённой параметр «Разрешить вход в систему через службу удаленных рабочих столов.»

3.6. Журналы событий Windows

В MicrosoftWindows *событие (event)* – это любое происшествие в операционной системе, которое записывается в журнал или требует уведомления пользователей или администраторов.

Приложение «Просмотр событий» можно открыть следующим способом: «Пуск», «Панель управления», из списка компонентов панели управления выбирать «Администрирование» и из списка административных компонентов стоит выбрать «Просмотр событий»;

Стандартный набор включает 3 журнала: Приложение, Безопасность, Система.

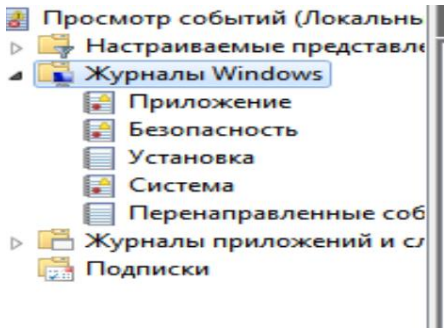

Рисунок 21 - Стандартные журналы

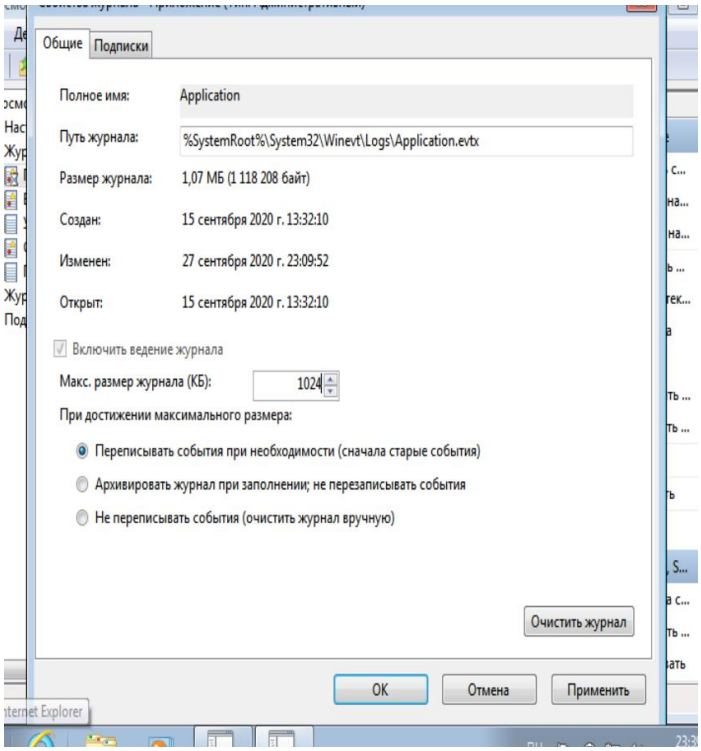

Рисунок 22 - Изменение свойств журнала

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

В результате лабораторной работы была произведена настройка локальных политик безопасности АРМ с установленной ОС Windows 7 и расположенного в «открытом» и «закрытом» контурах («закрытый» контур имел тип 1Б).