1 Цель

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). В данной работе использовалась Windows 7 x64.

2 Краткие теоретические сведения

Нарушение базовых услуг безопасности "конфиденциальность", "целостность" и "доступность" ресурсов АРМ может нанести непоправимый ущерб как самой ИС, так и организации, использующей её.

Существуют АРМ "открытого" и "закрытого" контуров. "Закрытый" контур характеризуется наличием секретной информации, получение НСД к которой опасно для деятельности организации. "Открытый" контур АРМ обладает общедоступной информацией. Для "закрытого" контура АРМ предъявляются повышенные требования безопасности.

Подсистема защиты АРМ от НСД "закрытого" и "открытого" контура должна обеспечивать: однозначную идентификацию пользователей в ИС и в операционной системе АРМ. Завершение работы пользователя АРМ должно сопровождаться освобождением всех занимаемых им разделяемых ресурсов (Logout), а все носители проверяться на наличие вирусов.

АРМ "открытого" и "закрытого" контура ИС должны защищаться от НСД с помощью сертифицированной системы защиты информации (СЗИ). В минимальной конфигурации СЗИ от НСД должны обеспечивать:

- создание изолированной программной среды (ИПС) на АРМ, обеспечивающей возможность запуска только заданного набора программ и/или процессов.

- идентификацию и аутентификацию пользователей, предоставление доступа к ресурсам компьютера только по предъявлению личного аппаратного идентификатора и пароля.

- контроль целостности программных средств СЗИ от НСД до входа пользователя в ОС.

- Разграничение доступа к локальным каталогам и файлам рабочей станции, обеспечивающее защиту от модификации системного и прикладного ПО АРМ.

- регистрацию попыток входа в систему и попыток доступа к важнейшим объектам локальной файловой системы.

- блокировку работы пользователей в случае нарушения ограничений, наложенных СЗИ от НСД.

Локальные политики безопасности АРМ – это набор параметров безопасности ОС Windows и СЗИ от НСД, которые обеспечивают безопасность АРМ в соответствии с требованиями политики информационной безопасности ИС организации.

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

Таблица 2.1

Наименование запрета	Пояснения
Запрет загрузки с внешних носителей	Пользователю запрещается осуществлять загрузку компьютера с системной дискеты или с загрузочного CD ROM 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

Наименование запрета	Пояснения
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 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

3 Ход работы

Тип ИС закрытого контура — 1В.

3.1 Подготовка к настройке локальных политик безопасности

3.1.1 Установка макета варианта лабораторной работы была проведена

установка среды виртуализации VirtualBox v6.1.10

3.1.2 Переход к настройкам локальных политик безопасности

В меню "Пуск" в поле поиск было найдено и запущено приложение Локальная политика безопасности.

3.2 Управление встроенными учетными записями

Встроенными учетными записями являются учетные записи гостя и администратора. Они обладают различными правами в системе. Так, например, гость не может менять настройки и не имеет доступа к данным.

Для того, чтобы переименовать гостевую учётную запись перейдём в приложении "Локальная политика безопасности" в узел "Локальные политики" → "Параметры безопасности" → "Учетные записи: Состояние учётной записи Гость" и активировать её.

Затем перейдём в "Учетная запись": Переименование учётной записи "гостя" и в открывшемся окне напишем "Гостевая запись".

После чего перезагрузим компьютер.

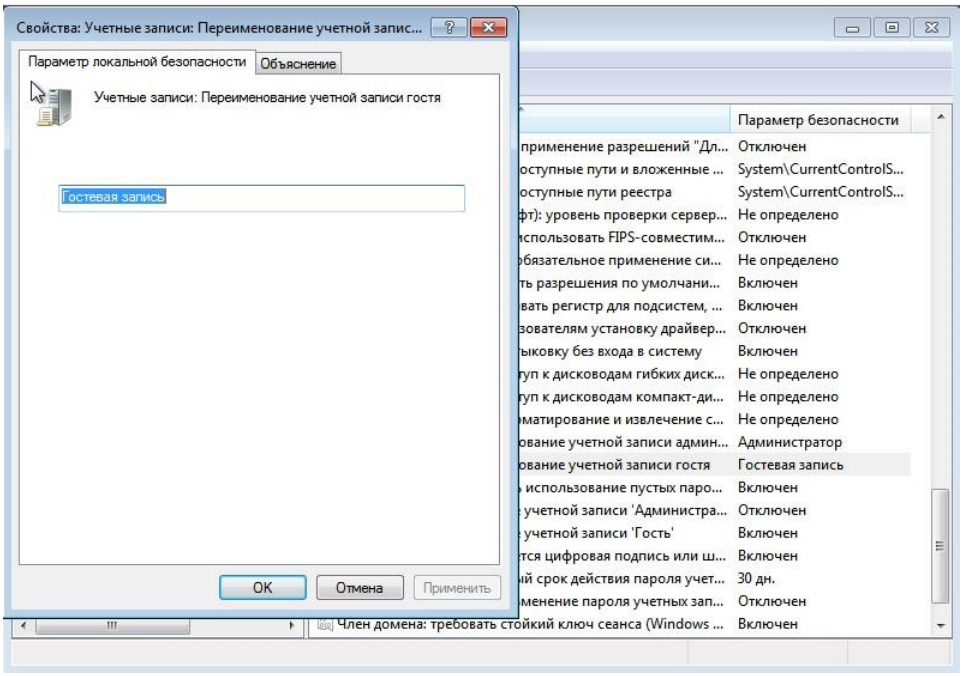

Рис. 1: Переименование учётной записи гостя

Включение гостевой записи не будет противоречить требованиям для данного контура, так как класс защищенности 1В находится в первой группе, которая включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС.

3.3 Управление политиками паролей

Одним из ключевых пунктов безопасности АРМ в ИС является политика паролей. Правильная её настройка значительно усложняет НСД в ИС. К этим правилам относится:

1. *Вести журнал паролей* — данная опция позволяет администратору узнать какие пароли были установлены до этого и организовать действия по улучшению безопасности.

2. *Максимальный срок действия пароля* — устанавливает максимальное время, которое может использоваться текущий пароль.

3. *Минимальная длина пароля* — устанавливает минимальное кол-во символов пароля.

4. *Минимальный срок действия пароля* — устанавливает время, в течении которого нельзя повторно изменить пароль. Позволяет избежать ситуации, когда пользователь после обязательной смены пароля тут же менял его на предыдущий.

5. *Пароль должен отвечать требованиям сложности* — данная опция обязывает пользователя создавать пароли с буквами различного регистра, цифрами, а также специальными символами, такими как !, *, – и др.

6. *Хранить пароли используя обратимое шифрование* — после включения данной опции все пароли системы будут хранится в зашифрованном виде в системе. Это уменьшает безопасность ИС, т.к. изначально хранится только хэш-код пароля.

Для установки данных требований нужно перейти Локальная политика безопасности → Параметры безопасности → Политика учётных записей → Политика паролей.

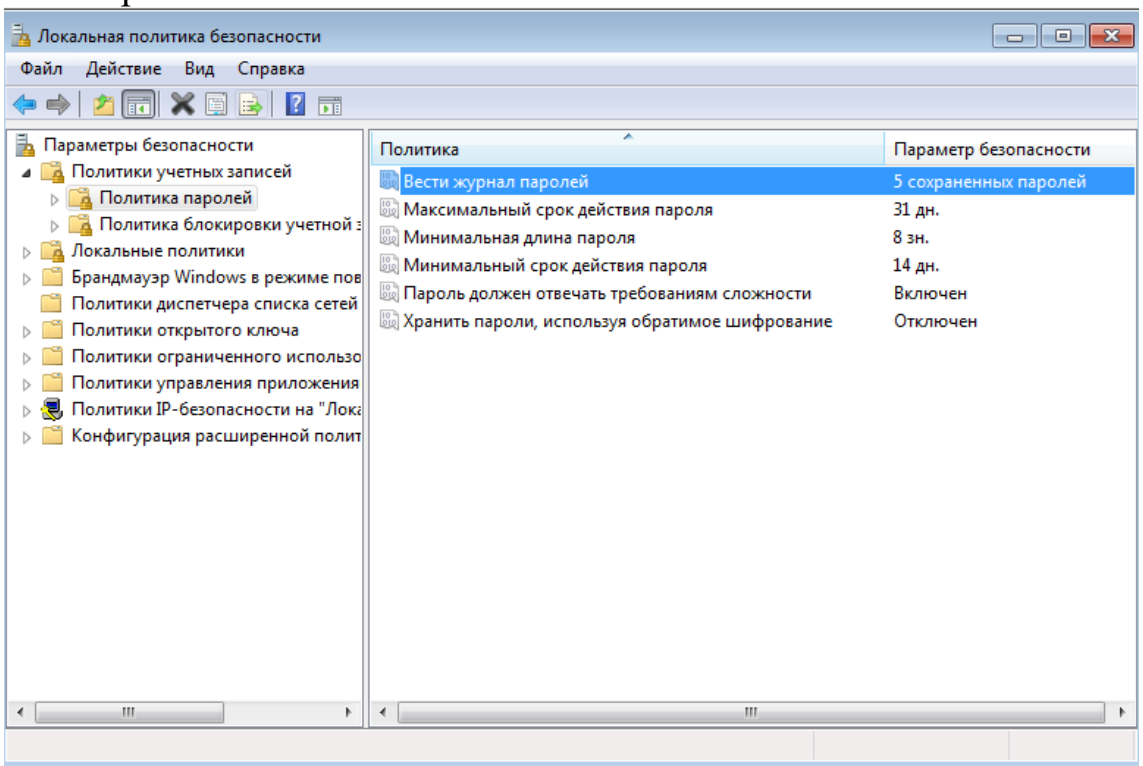

Рис. 2: Политика паролей

Была установлена политика паролей на Рис. 2 исходя из нормативных документов ФСТЭК и типа ИС закрытого контура 1В. Согласно требованиям к классу защищенности 1В, должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Кроме того, для дополнительной устойчивости к паролям также будет выдвигаться требование сложности

3.4 Политика блокировки учётной записи

Даже после правильной настройки политики безопасности учётные записи пользователей всё ещё могут быть подвергнуты атакам злоумышленников. Обладая достаточными ресурсами и навыками, хакеру может хватить времени для подбора пароля к учётной записи. Для противостояние таким действиям существует "Политика блокировки учётной записи". Данная политика включает в себя:

1. *Время до сброса счётчика блокировки* — этот параметр определяет время, после которого кол-во неудачных попыток сбросится в ноль.

2. *Пороговое значение блокировки* — определяет кол-во некорректных попыток входа, после чего учётная запись будет заблокирована.

3. *Продолжительность блокировки учётной записи* — определяет время, в течении которого будет заблокирована учётная запись.

Для установки данных требований нужно перейти Локальная политика безопасности → Параметры безопасности → Политика учётных записей → Политика блокировки учётных записей.

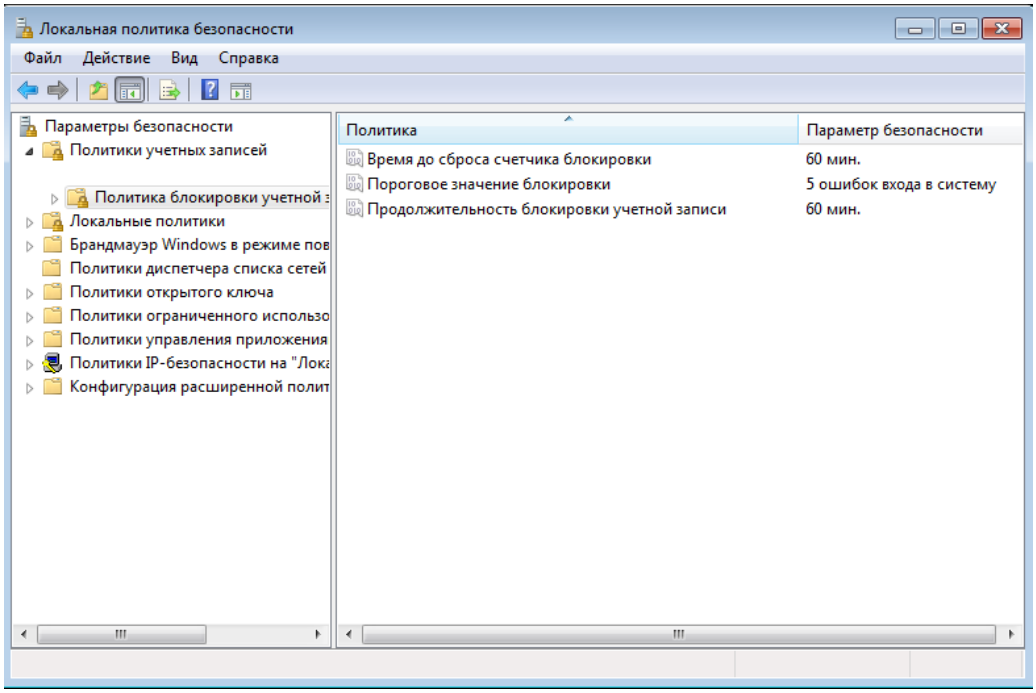

Рис. 3: Политика блокировки учётных записей

Система позволяет пользователю 5 раз ошибиться с паролем. Продолжительность блокировки установлено в 60 минут. Этого достаточно, чтобы администратор и команда ИБ приняли все необходимые меры.

3.4 Политика аудита

С помощью политик аудита можно усовершенствовать безопасность АРМ. Политика аудита — это совокупность параметров, определяющих какая информация будет поступать в журнал аудита АРМ. Данная политика включает следующие параметры:

1. *Аудит входа в систему* — аудит каждой попытки входа пользователя в систему или выход из неё. Успех означает аудит каждой успешной попытки, а отказ — каждой неудачной.

2. *Аудит доступа к объектам* — аудит попыток доступа к файлам, папкам, принтерам, разделам системного реестра, к объектам, которые не имеют отношения к ActiveDirectory.

3. *Аудит доступа к службам каталогов* — аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне "Дополнительные параметры безопасности".
4. *Аудит изменения политики* — аудит каждого изменения политики назначения прав пользователям, учетной записи или доверия.

5. *Аудит использования привилегий* — аудит использования привилегий и прав пользователя.

6. *Аудит отслеживания процессов* — аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам.

7. *Аудит системных событий* — благодаря ей можем 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 вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени.

8. *Аудит событий входа в систему* — аудит проверки компьютером учётных данных, подключение к данным членов домена.

9. *Аудит управления учётными записями* — аудит каждого события управления учётными записями на компьютере: создание, перемещение и отключение учётных записей, а также изменение паролей и групп.

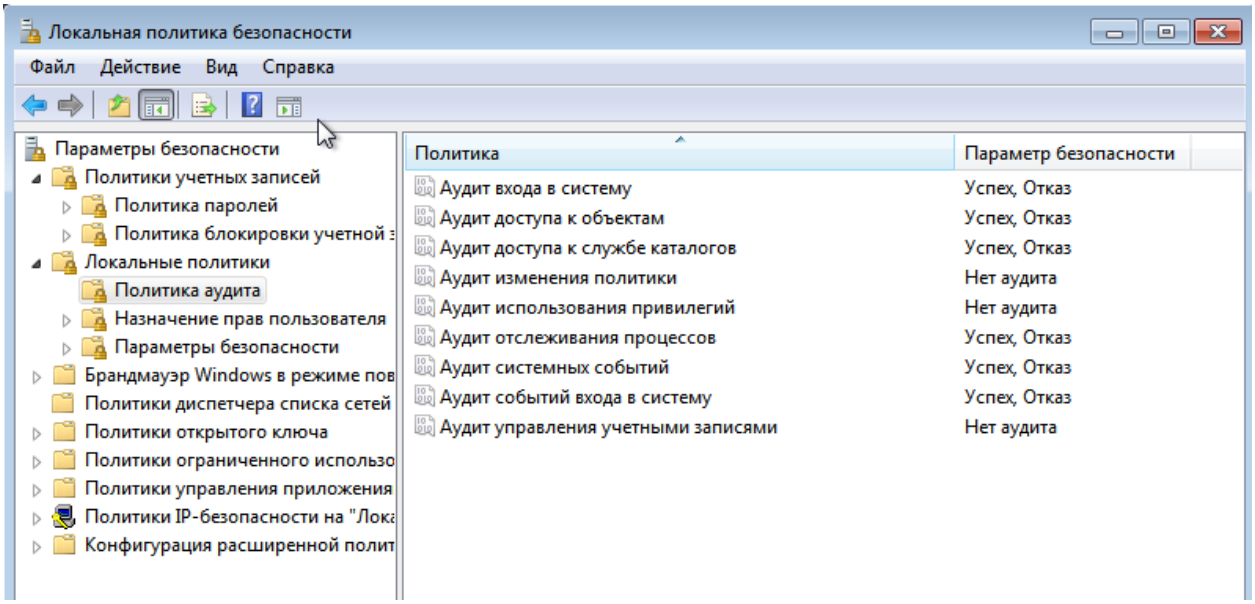

Рис. 4: Настроенная политика аудита

Данные параметры выставлены в соответствии с вариантом: тип ИС закрытого контура 1В.

3.5 Политика назначения прав пользователей

Обычные пользователи не владеют достаточной базой знаний по обеспечению безопасности и могут "случайно" нанести вред ИС. Чтобы избежать этого существует политика назначения прав пользователя, которая включает в себя 44 параметры. Вот некоторые из них:

1. *Добавление рабочих станций к домену* — отвечает за разрешение пользователям или группам добавлять компьютеры в домен ActiveDirectory.

2. *Доступ к компьютеру из сети* — отвечает за разрешение подключения к компьютеру по сети указанным пользователям или группам.

3. *Завершение работы системы* — указывает список пользователей, которые имеют право на использование команды "Завершение работы" после удачного входа в систему.

4. *Запрет входа в систему через службу удалённых рабочих столов* — ограничивает пользователям или группе вход в систему в качестве клиента удалённых рабочих столов.

5. *Запретить локальный вход* — запрещает отдельным пользователям или группам выполнять вход в систему.

6. *Изменение системного времени* — отвечает за разрешение пользователям или группам менять системное время.

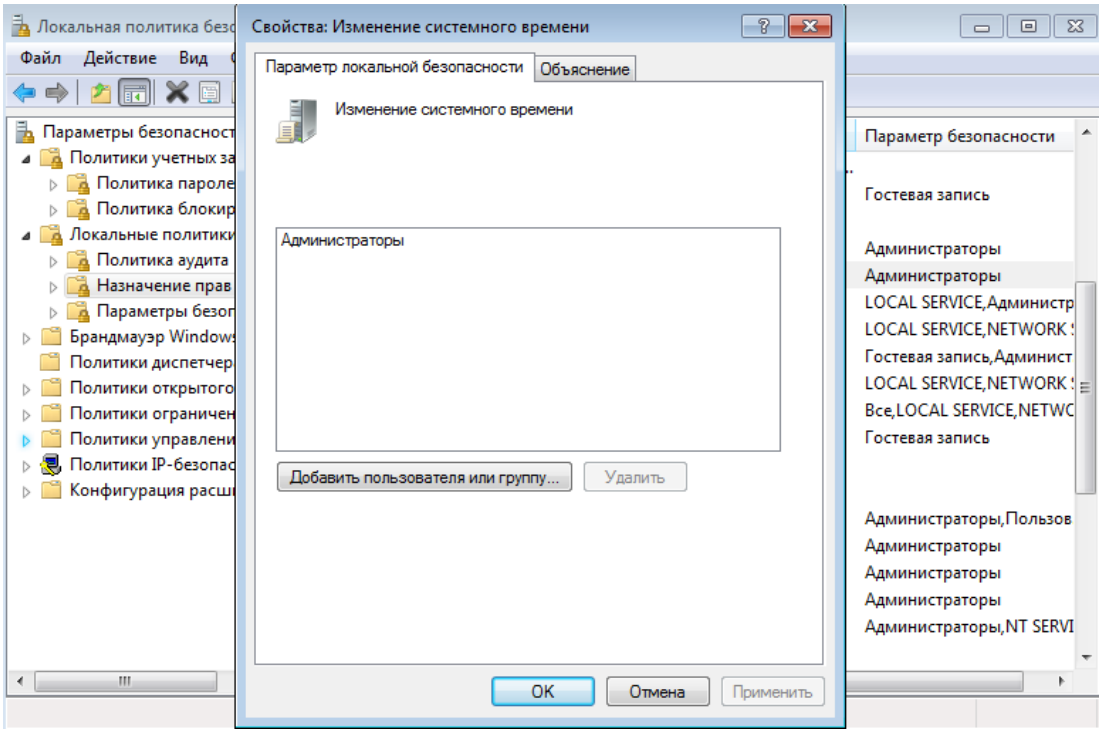

Рис. 5 Изменение системного времени

Так как изменение системного времени является операцией, которая может серьезно повлиять на работоспособность системы, то были удалены все ненужные группы пользователей из списка тех групп, которые могут выполнять данное действие.

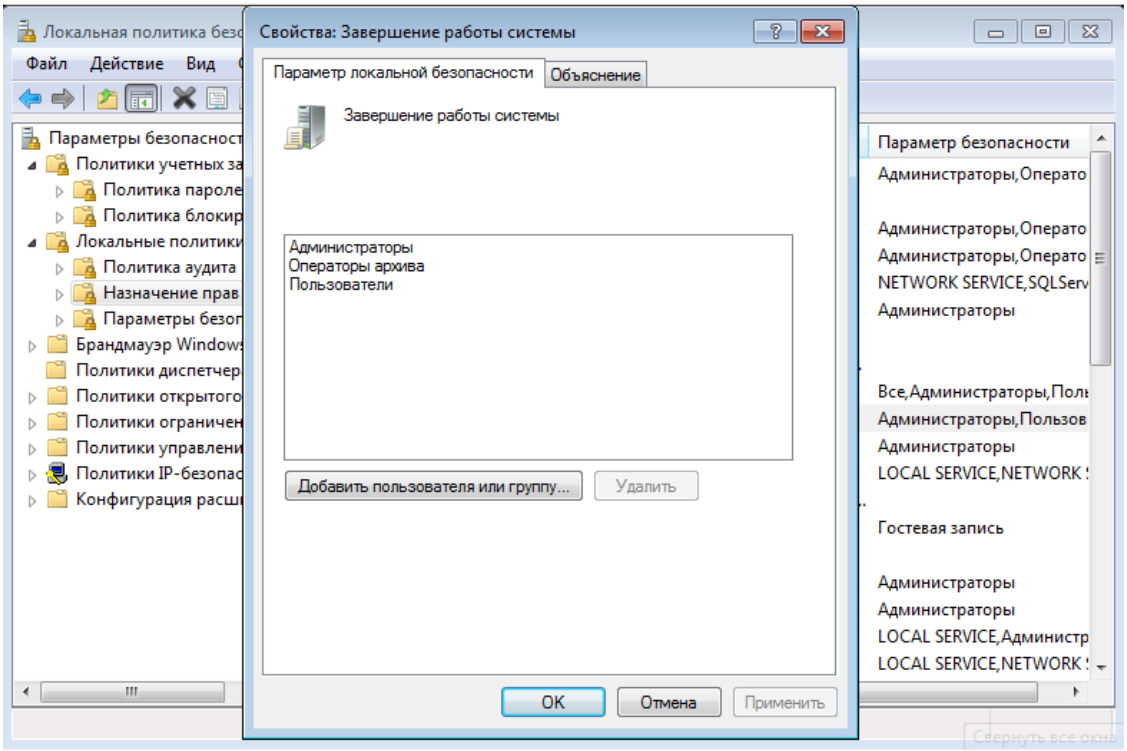

Рис. 6 Завершение работы системы

Параметр Завершение работы был оставлен без изменений. Эта операция должна быть доступна всем пользователям, которые имеют доступ на вход в систему.

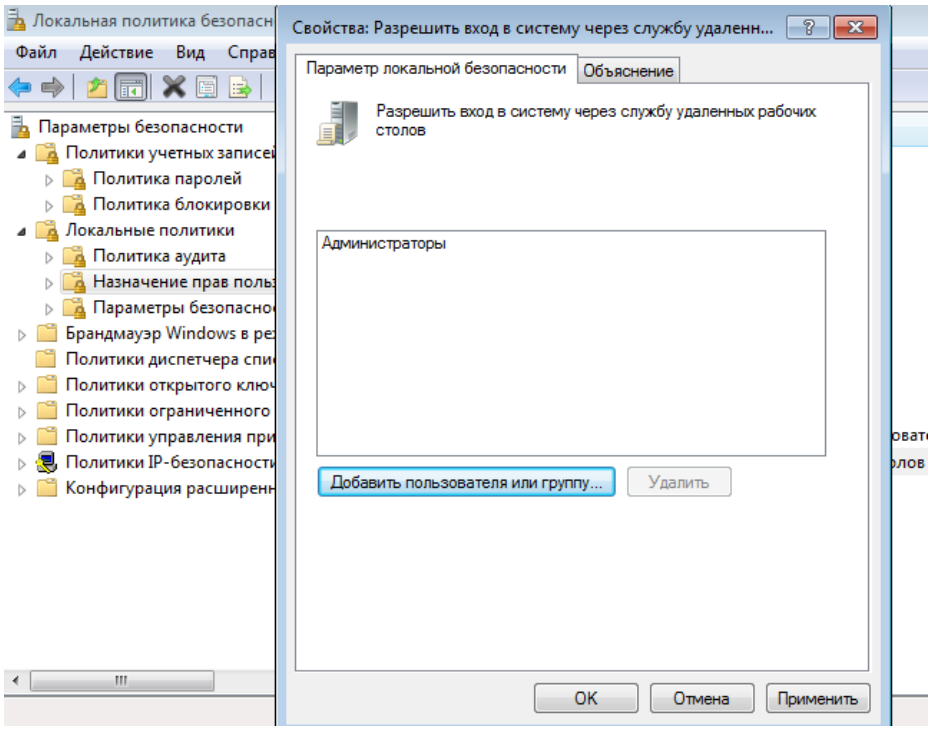

Рис. 7 Разрешить вход в систему через службу удалённых рабочих столов

Так как вход в систему через службу удаленных рабочих столов является операцией, которая может серьезно повлиять на работоспособность системы, и данный контур подразумевает наличие администратора (службы) защиты информации в АС (требование 4.3 к АС первой группы), то была удалена группа «Пользователи удаленного рабочего стола» из списка тех групп, которые могут выполнять данное действие (рисунок 7).

3.6 Журнал событий Windows

В ОС Windows любое происшествие – событие – записывается в журнал или выводится администратору, или пользователю. Эти журналы представляют важные хронологические сведения, помогающие вести мониторинг системы. Для просмотра журнала необходимо открыть "Панель управления" и выбрать категорию "Крупные значки" и в списке найти "Администрирование". Затем перейти в "Просмотр событий". Стандартный набор включает:

1. *Приложение* — хранит важные события, связанные с конкретным приложением.

2. *Безопасность* — хранит события, связанные с безопасностью. Например, вход/выход из системы.

3. *Система* — хранит события операционной системы или её компонентов, например, неудачи при запуске служб или инициализации драйверов.

К классу защищённости 1В выдвигаются требования о регистрации входа (выхода) субъектов доступа в (из) систему (узел сети), либо регистрация загрузки и инициализации операционной системы и ее программного останова.

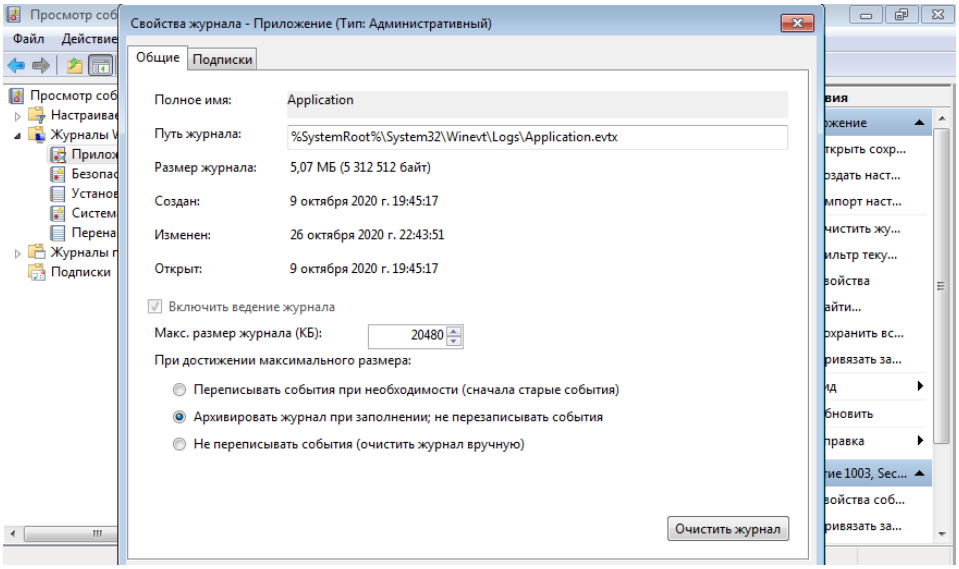

Рис. 8: Свойства журнала событий Приложение

Такие же параметры установлены для журналов Безопасность и Система.

4 Выводы

Подсистема защиты от НСД и правильная настройка её политик способно значительно повысить безопасность ИС от НСД. А также предоставляет спектр возможностей по анализу и совершенствованию текущей СЗИ.

В данной лабораторной работе была проведена настройка локальных политик безопасности АРМ в соответствии с типом ИС закрытого контура 1В.
Также ознакомились с журналом событий Windows и его свойствами.