Цель работы: изучить и научиться настраивать локальные политики безопасности на автономном автоматизированном рабочем месте (АРМ) пользователя с установленной на нем операционной системой Windows для защиты информации от несанкционированного доступа (НСД).

Требования к классу защищенности 1Д

Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. Согласно данному нормативному документу требования к классу защищенности 1Д следующие:

1.1 Подсистема управления доступом

Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

1.2 Подсистема регистрации и учета

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. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная - несанкционированная; идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

1.3 Подсистема обеспечения целостности

Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;
- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Настройка политик

2.1 Управление встроенными учетными данными

Из меню пуска открываем ***панель управления*** и затем выбираем ***учетные записи пользователей***. Как видно, есть две учетные записи: администратор и гость.

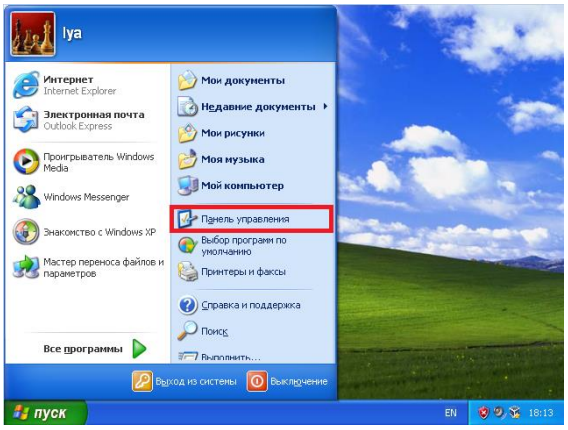

Рисунок 1 - Панель управления

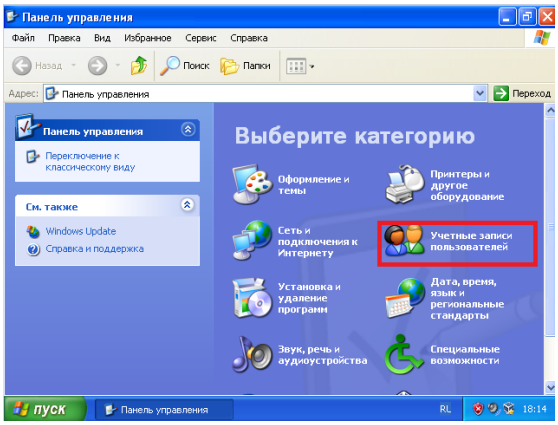

Рисунок 2 - Учетные записи пользователей

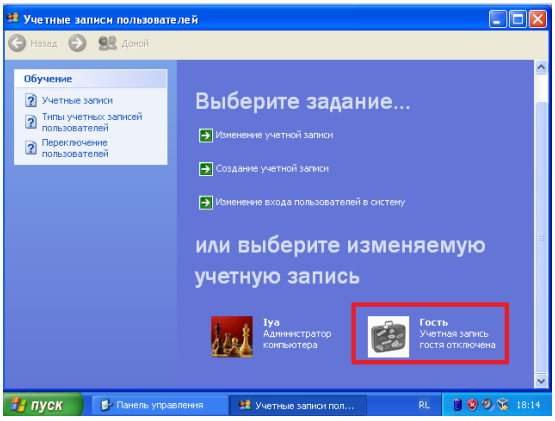

Рисунок 3 - Учетные записи пользователей

Необходимо переименовать гостевую учетную запись. Для этого, воспользовавшись комбинацией ***Win+R,*** введем ***secpol.msc***:

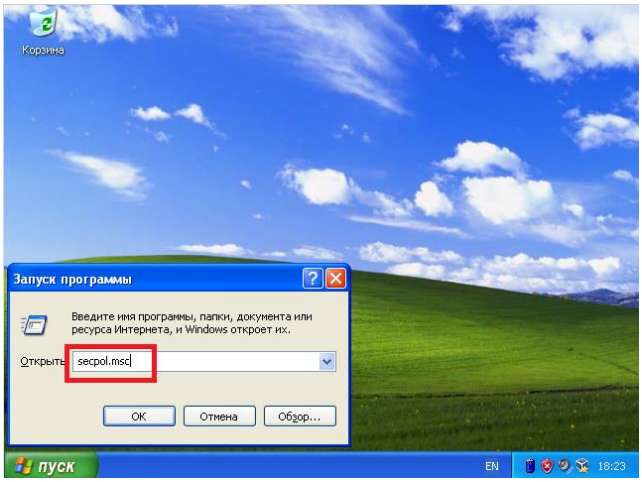

Рисунок 4 - secpol.msc

Затем перейдем в ***локальную политику безопасности*** и выберем ***параметры безопасности*:**

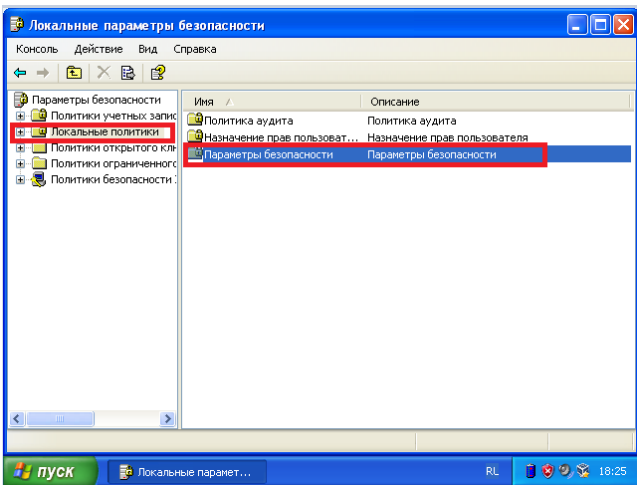

Рисунок 5 - Параметры безопасности

Выбирается ***учетные записи***: переименование учетной записи гостя:

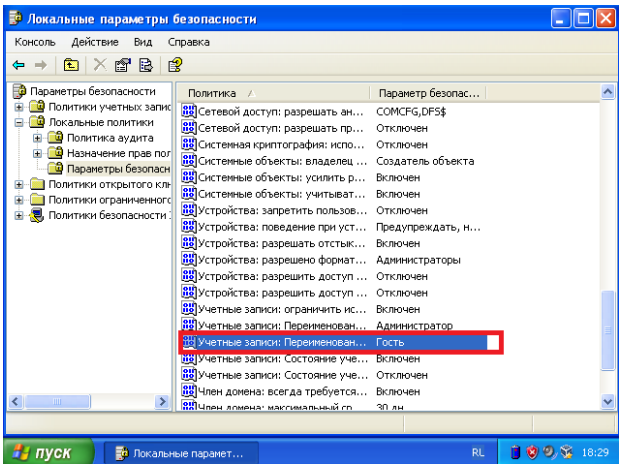

Рисунок 6 - Учетные записи гостя

Теперь переименуем название учетной записи. Это необходимо для того, чтобы посторонним лицам было бы намного труднее угадать новое имя пользователя и пароля учетной записи, так как по умолчанию учетная запись гость имеется на всех компьютерах Windows 2000 Server, Windows 2000 Professional, Windows XP Professional или Windows Server 2003.

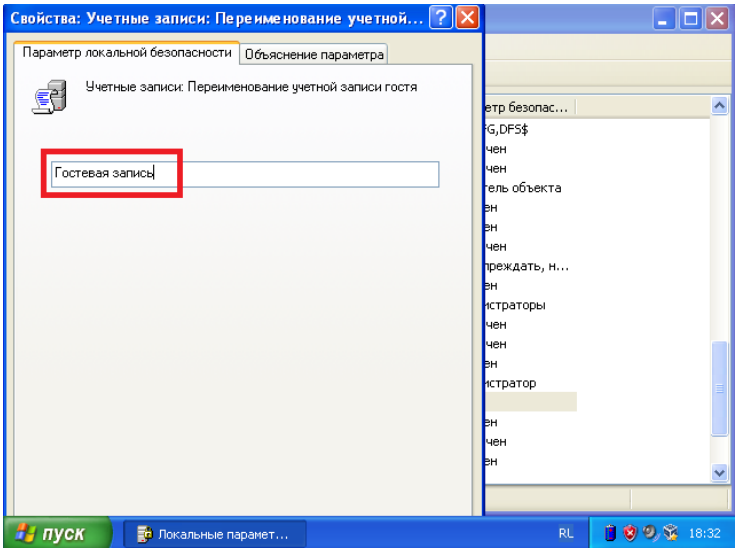

Рисунок 7 - Гостевая запись

Теперь аналогичным образом проверим имя записи и убедимся, что она переименована:

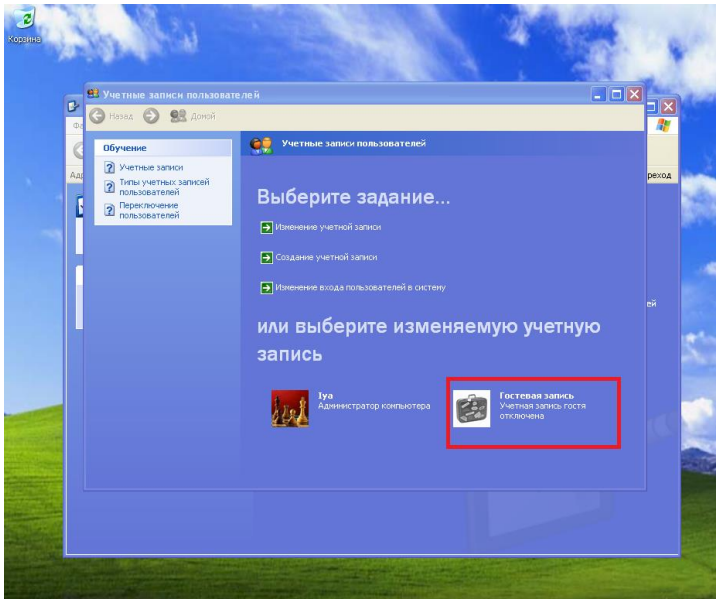

Рисунок 8 - Запись переименована

2.2 Управление политиками паролей

Доступно 6 политик безопасности, обеспечивающих проверку подлинности субъектов доступа. Опишем и настроим каждую из них.

2.2.1 Максимальный срок действия пароля

Доступные значения от 0 до 999 дней. Рекомендуемые значения от 30 до 45 дней.

2.2.2 Минимальная длина пароля

Согласно требованию к классу защищенности 1Д к подсистеме управления доступом, длина пароля должна быть не менее 6 буквенно-цифровых символов. Оптимальным значением для количества знаков для пароля пользователей является 8.

2.2.3 Минимальный срок действия пароля

Настраивается минимальное количество дней, в течение которого пользователь должен использовать свой новый пароль. Доступные значения этой политики устанавливаются в промежутке от 0 до 998 дней.

2.2.4 Требование сложности к паролям

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 учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

2.2.5 Неповторимость паролей

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

2.2.6 Хранение паролей с использованием обратимого шифрования

Обратимое шифрование по умолчанию отключено, так как, используя эту политику, уровень безопасности паролей и всего домена, в частности, значительно понижается.

Настроим все вышеописанные политики. Для этого воспользуемся комбинацией ***Win+R*** введем ***secpol.msc***:

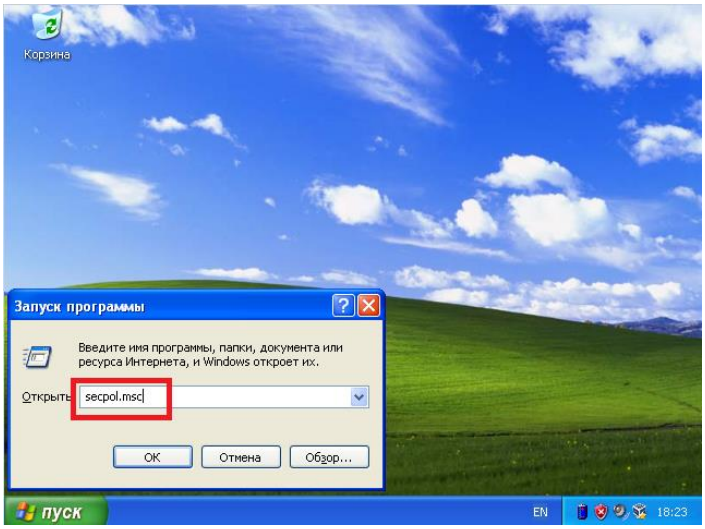

Рисунок 9 - secpol.msc

Затем перейдем в ***политику учетных записей*** и откроем параметр ***политика паролей***:

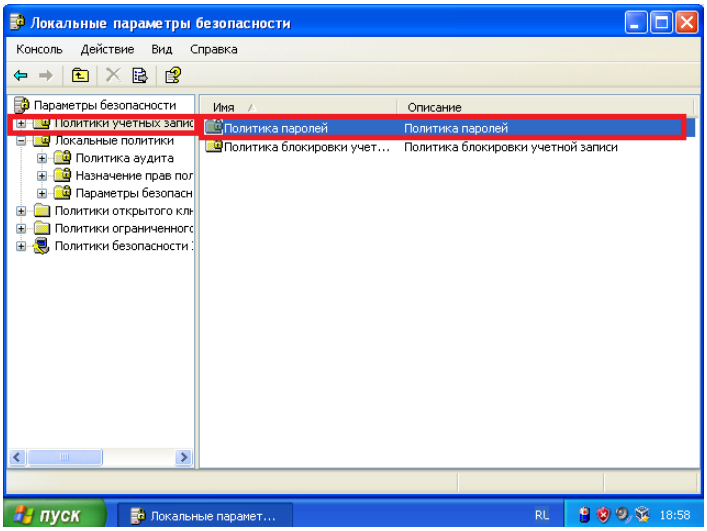

Рисунок 10 - Политика паролей

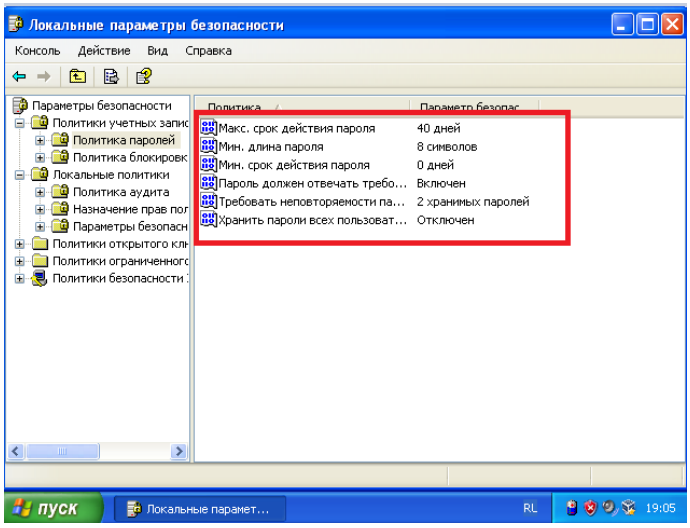

Рисунок 11 - Настройка политики паролей

2.3 Политика блокировки учетной записи

При помощи данного набора политик, у вас есть возможность ограничения количества некорректных попыток входа пользователя в систему с целью предотвращения попыток несанкционированного доступа. Доступны три политики. Рассмотрим и настроим каждую из них.

2.3.1 Время до сброса счетчиков блокировки

При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Допустимые значения от 1 минуты до 99999. Это значение должно быть меньше значения политики «Продолжительность блокировки учетной записи».

2.3.2 Пороговое значение блокировки

Используя эту политику, можно 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. Рекомендуется устанавливать допустимое количество от трех до семи попыток.

2.3.3 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.

Настроим все вышеописанные политики. Для этого, воспользовавшись комбинацией ***Win+R,*** введем ***secpol.msc***. Затем перейдем в ***политику учетных записей*** и выберем ***политику блокировки учетной записи***:

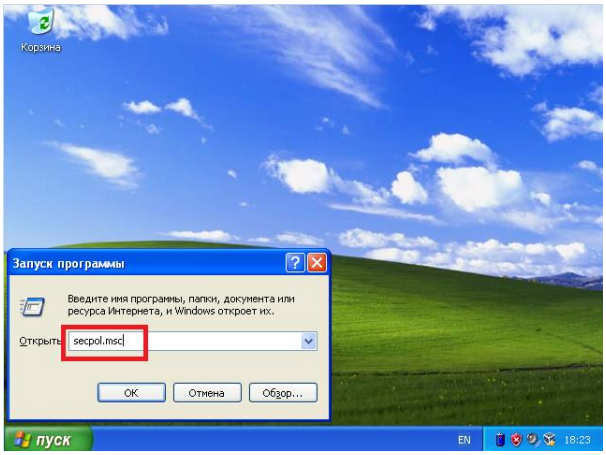

Рисунок 12 - secpol.msc

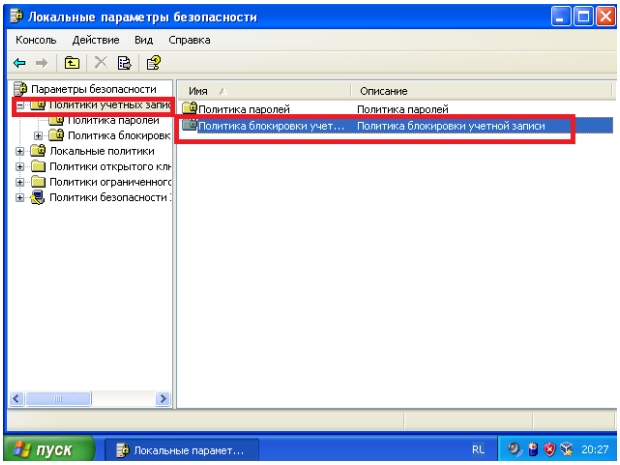

Рисунок 13 - Политика блокировки учетных записей

Настроим соответствующие политики:

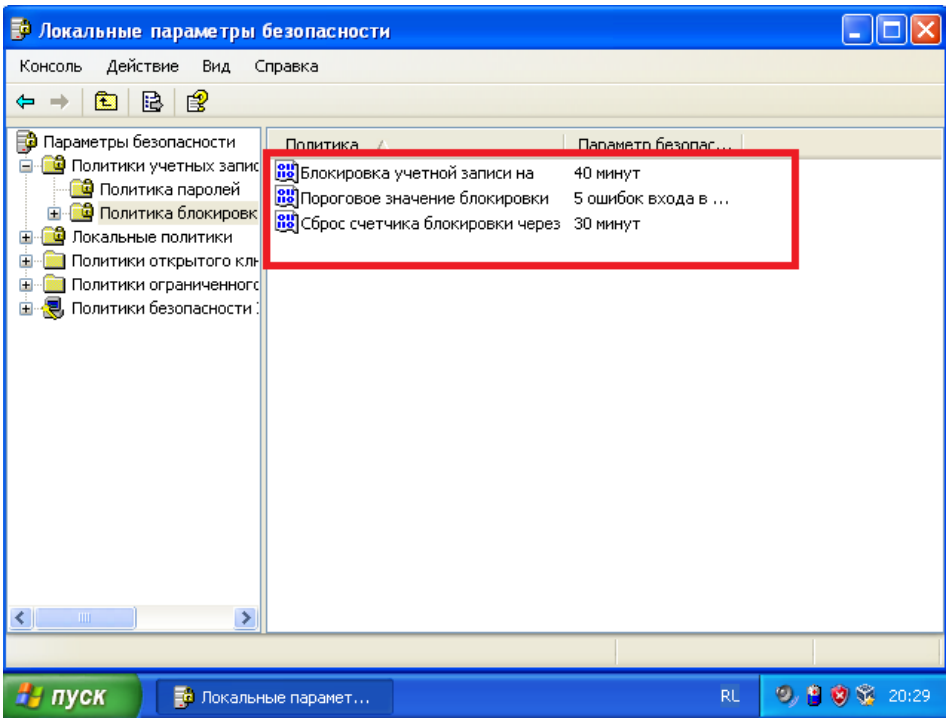

Рисунок 14 - Настройка политики блокировки учетных записей

2.4 Политика аудита

Согласно требованию нормативного документа 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. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная - несанкционированная; идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Доступно 10 следующих политик:

2.4.1 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 нее.

2.4.2 Аудит доступа к объектам

Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, например, файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом (SACL).

2.4.3 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 Active Directory. 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 Active Directory, для которого определена таблица SACL. Аудит

отказов означает создание записи аудита при каждой неудачной попытке доступа пользователя к объекту Active Directory, для которого определена таблица SACL.

2.4.4 Аудит изменения политики

Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики 6 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.

2.4.5 Аудит 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.

2.4.6 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.

2.4.7 Аудит 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.

2.4.8 Аудит 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.

2.4.9 Аудит 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 7 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.

Требования к классу защищенности 1Д включают не все политики, однако настроим все вышеописанные политики, что позволит определить, кто вносил изменения, и найти виновника, если подобные изменения привели к каким-либо плачевным для компании последствиям. Для этого воспользуемся комбинацией ***Win+R*** введем ***secpol.msc***. Зайдем в ***локальные политики*** и выберем ***политику аудита***:

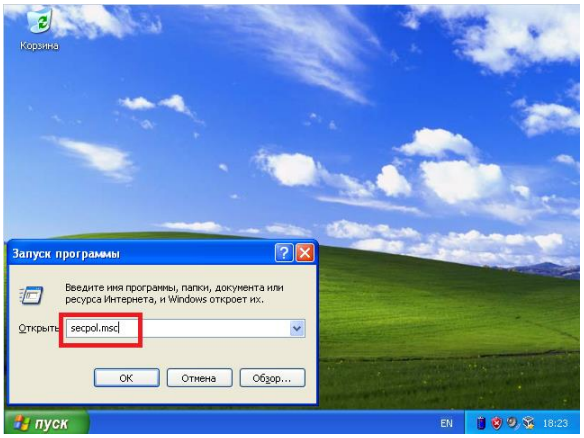

Рисунок 15 - secpol.msc

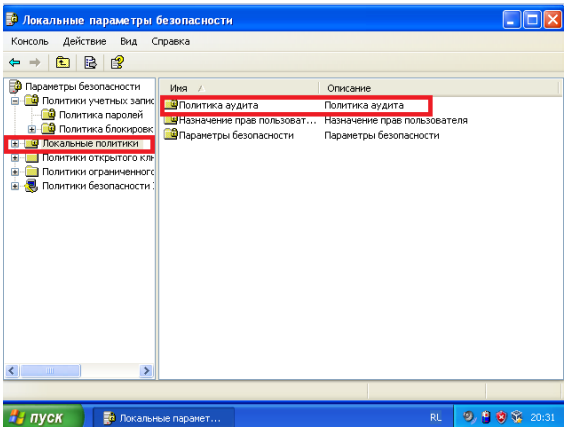

Рисунок 16 - Политика аудита

Настроим политики следующим образом:

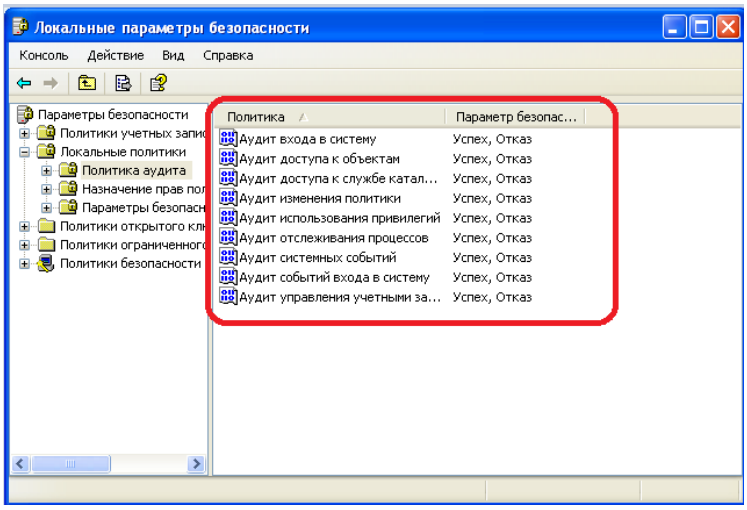

Рисунок 17 - Настройка политики аудита

2.5 Политика назначения прав пользователей

При помощи политик назначения прав пользователя вы можете сами определить, для каких пользователей или групп пользователей будут предоставлены различные права и привилегии, чтобы предотвратить намеренный или случайный ущерб системе.

Для назначения прав доступны 44 политики безопасности. Рассмотрим некоторые из политик:

2.5.1 Добавление рабочих станций к домену

Эта политика отвечает за разрешение пользователям или группам добавлять компьютеры в домен Active Directory. 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.

2.5.2 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».

2.5.3 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).

2.5.4 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.

2.5.5 Запретить локальный вход

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

2.5.6 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».

Настроим политики. Для этого, воспользовавшись комбинацией ***Win+R,*** введем ***secpol.msc***. Перейдем в ***локальные политики*** и выберем ***назначение прав пользователя***:

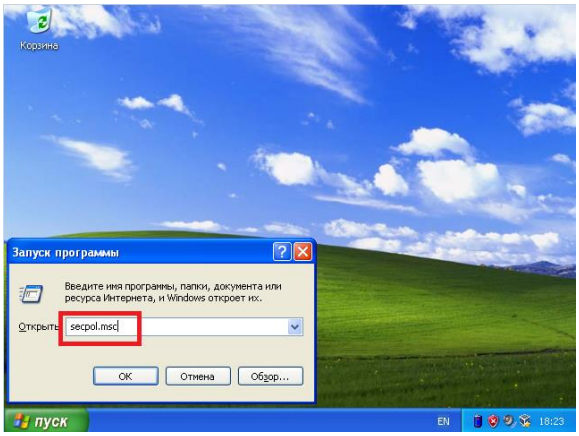

Рисунок 18 - secpol.msc

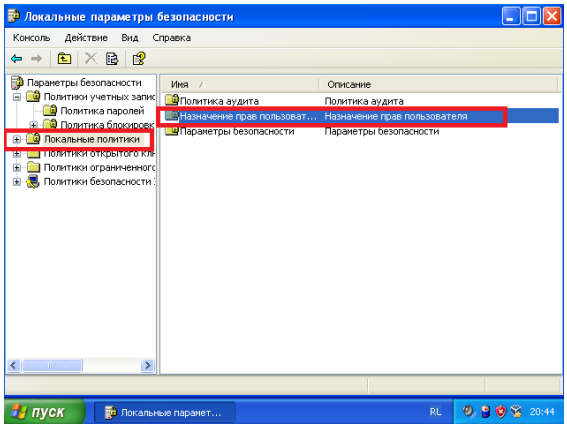

Рисунок 19 - Назначение прав пользователя

Настройка политик имеет вид:

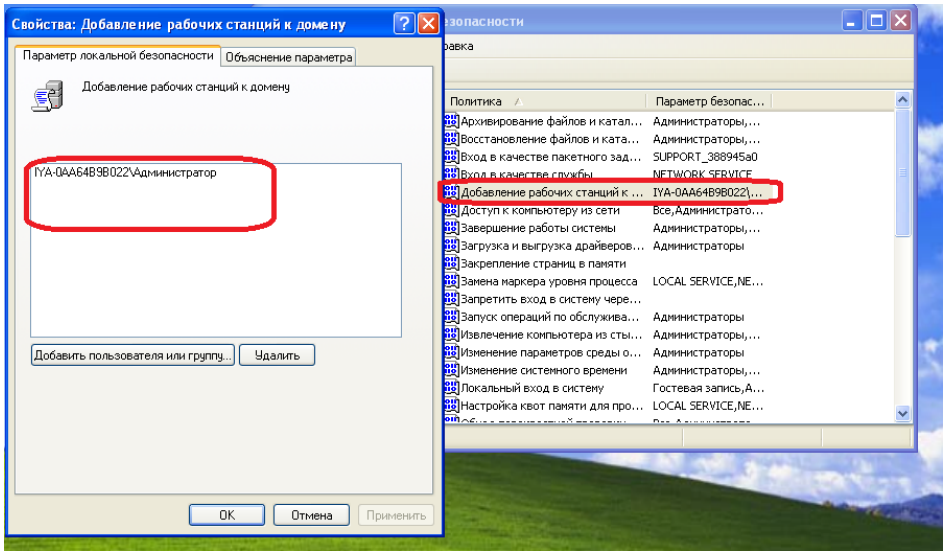

Рисунок 20 - Добавление рабочих станций к домену

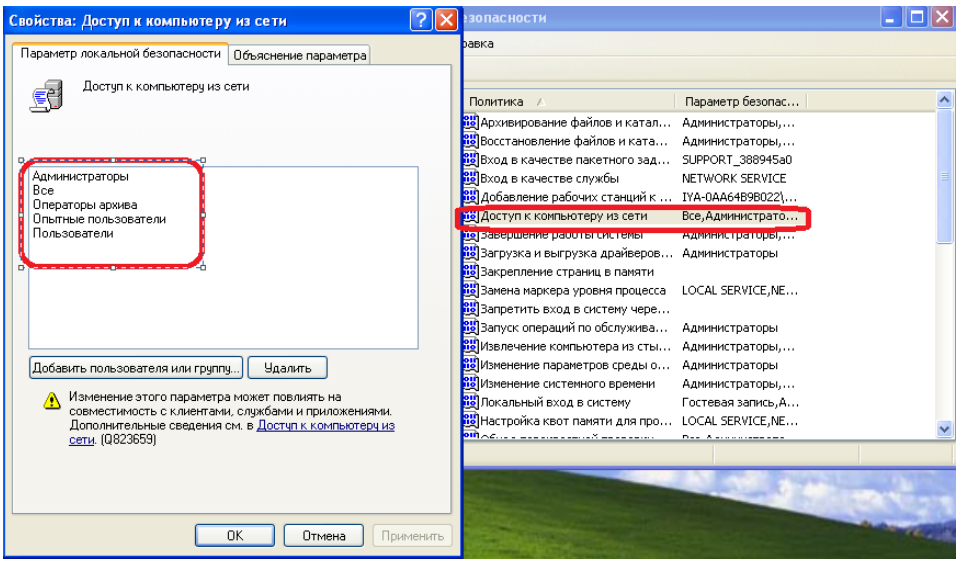

Рисунок 21 – Настройка доступа к компьютеру из сети остается без изменений

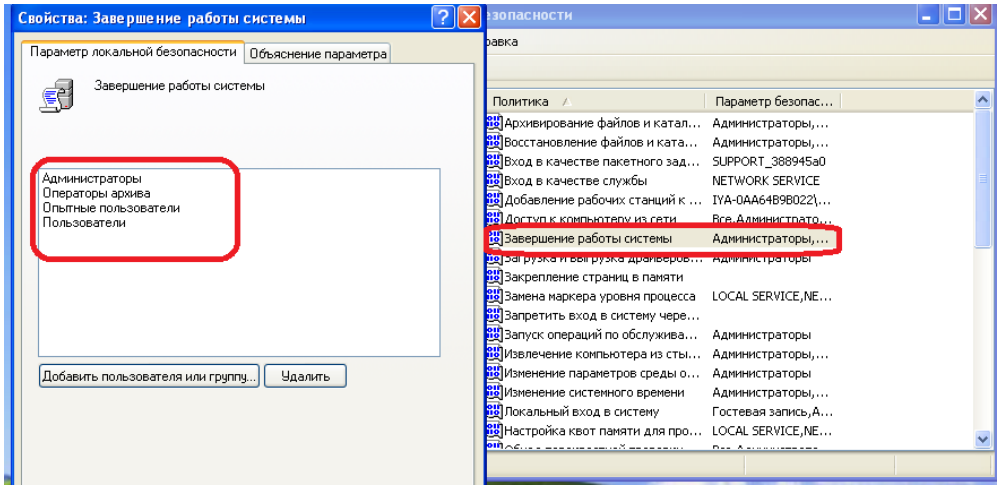

Рисунок 22 - Настройка завершения работы системы остается без изменений

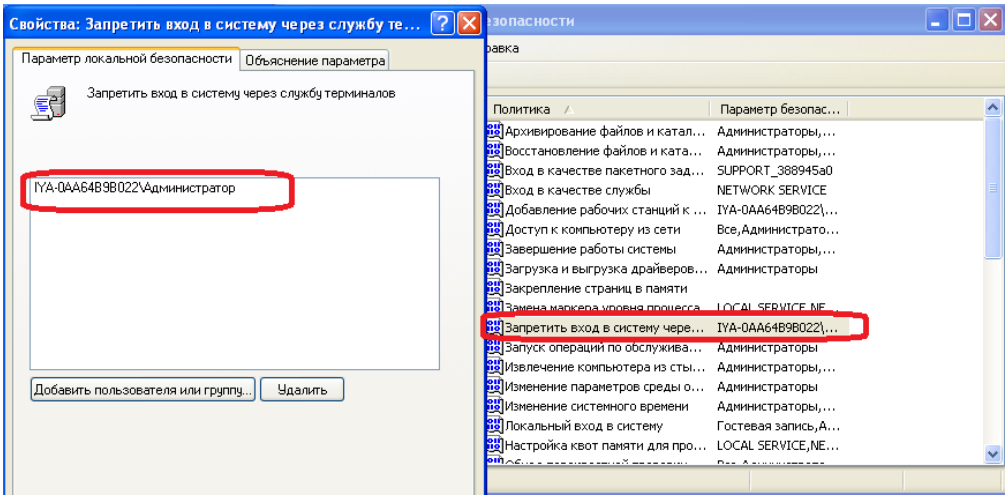

Рисунок 23 - Запрет входа в систему через службу удаленного доступа

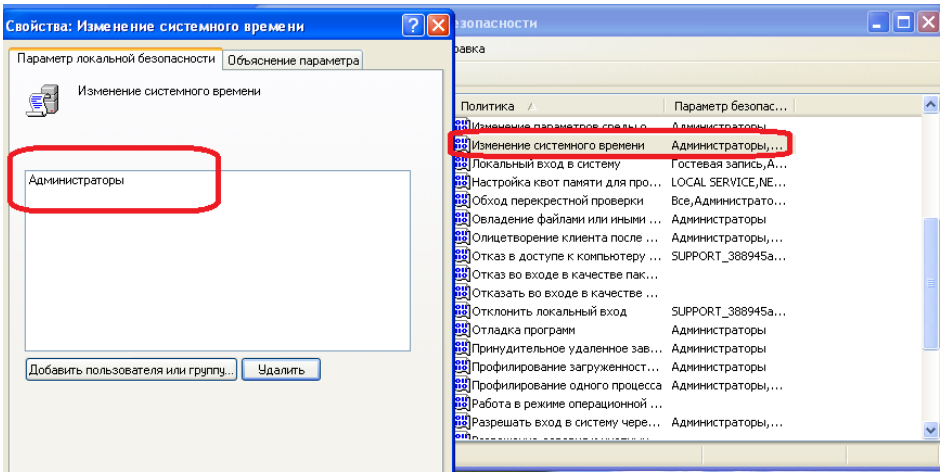

Рисунок 24 - Настройка изменения системного времени

2.6 Журнал событий Windows

Настройка данной политики обеспечивает регистрацию важных событий с целью мониторинга системы для поддержания ее безопасности, устранения ошибок и даигностики. Стандартный набор включает 3 журнала:

2.6.1 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.

2.6.2 Безопасность

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

2.6.3 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.

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.

Настроим все необходимый поля и журналы. Для этого нажмем ***пуск*** и перейдем в ***панель управления.*** Затем перейдем в ***администрирование*** и выберем ***просмотр событий***. Настроим следующим образом:

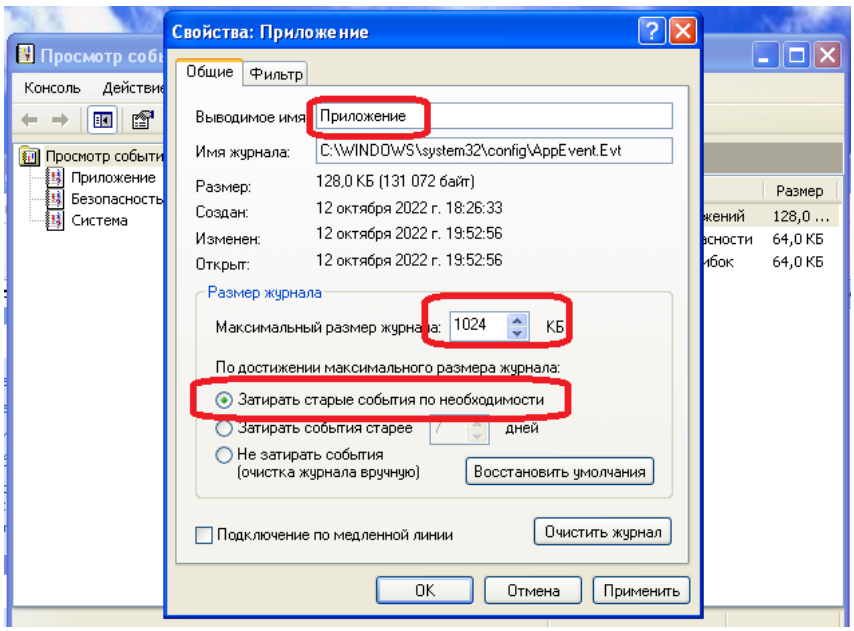

Рисунок 25 - Настройка журнала приложений

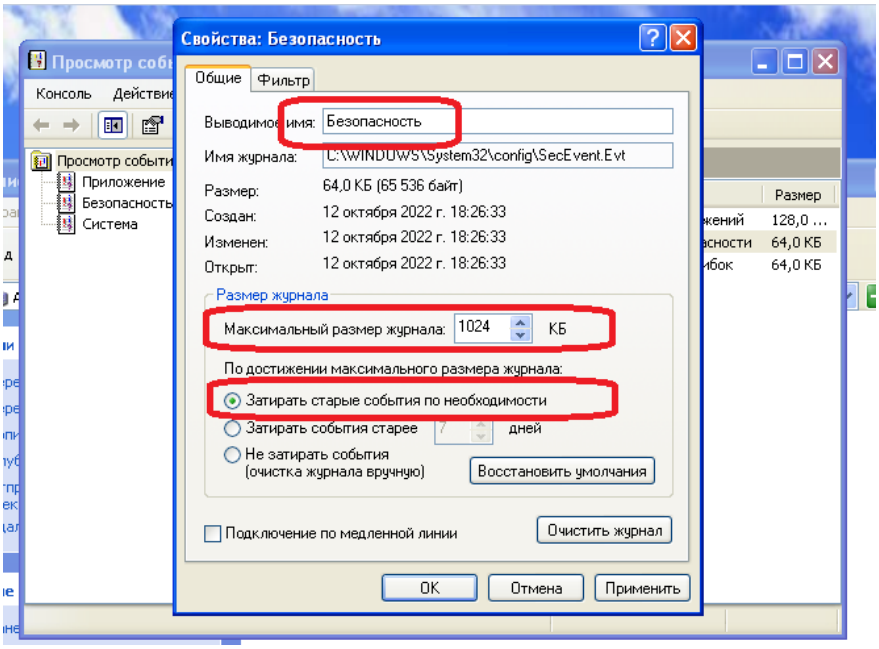

Рисунок 26 - Настройка журнала безопасности

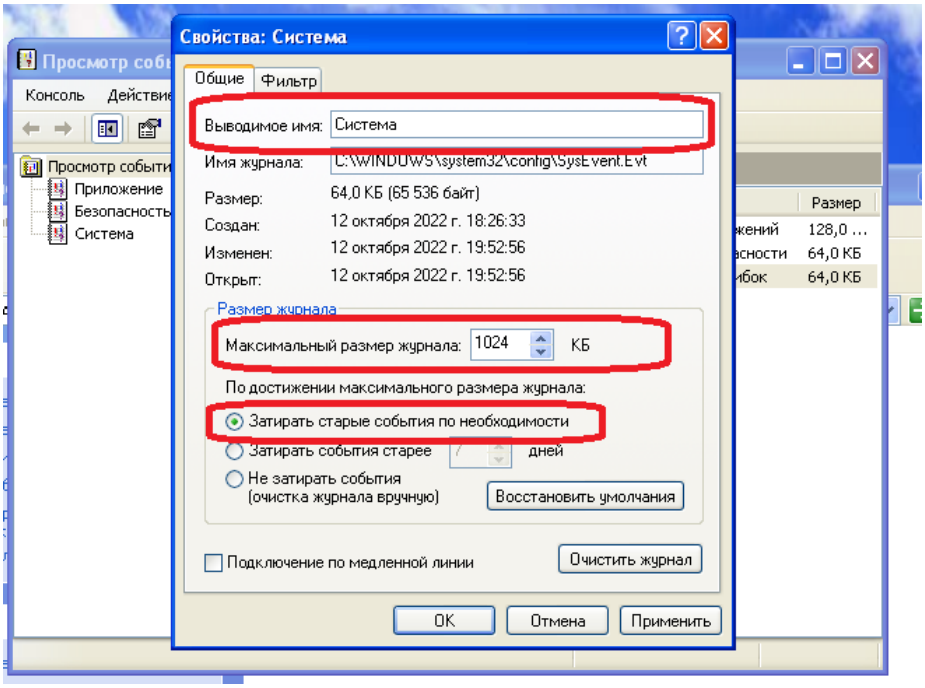

Рисунок 27 - Настройка журнала системы

Выводы: в ходе выполнения лабораторной работы были изучены и настроены локальные политики безопасности на АРМ пользователя с установленной на нем операционной системой Windows XP для защиты информации от несанкционированного доступа (НСД) с учетом требований ИБ к ИС класса 1Д, также был изучен нормативный документ ФСТЭК.

В рамках политики управления встроенными учетными данными была переименована и отключена гостевая запись с целью затруднения угадывания имени учетной записи.

В рамках управления политиками паролей был изменен максимальный срок действия пароля, минимальная длина пароля, минимальный срок действия пароля, установлены требования сложности к паролям и неповторимости, а также настроено хранение паролей с использованием обратимого шифрования. Все это было настроено по требованию к классу защищенности 1Д с целью проверки подлинности субъектов доступа.

В рамках политики блокировки учетной записи было настроено время до сброса счетчиков блокировки, установлено пороговое значение блокировки и продолжительность блокировки учетной записи с целью предотвращения попыток несанкционированного доступа.

В рамках политики аудита был настроен аудит входа в систему, аудит доступа к объектам, аудит доступа к службе каталогов, аудит изменения политики, аудит изменения политики, аудит изменений привилегий, аудит отслеживания процессов, аудит системных событий, аудит событий входа в систему с целью и настроен аудит управления учетными записями

по требованиям к классу защищенности 1Д, а также определения активности с целью принятия при необходимости дополнительных мер по обеспечению безопасности.

В рамках политики назначения прав пользователя было настроено добавление рабочих станций к домену, доступ к компьютеру из сети, управление завершением работы системы, запрет входа в систему через службу удаленных рабочих столов и запрет изменения системного времени с целью ограничение привилегий пользователя для предотвращения нанесения случайного или умышленного ущерба системе.

В рамках политики журналов событий было настроено три журнала с целью ведения мониторинга для поддержания безопасности.