МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «СГУ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

УТВЕРЖДАЮ
Заведующий кафедрой
д. ф.-м. н., доцент

_____ М. Б. Абросимов

ОТЧЕТ О ПРАКТИКЕ

студента 5 курса
факультета компьютерных наук и информационных технологий
Серебрякова Алексея Владимировича

Эксплуатационная практика
(Производственная практика)

кафедра теоретических основ компьютерной безопасности и криптографии
курс *пятый*
семестр *девятый*
продолжительность *4 недели, с 22 июня 2023 г. по 19 июля 2023 г.*

Руководитель практики
доцент к. ю. н., доцент А. В. Гортинский
личная подпись, дата

Саратов
2023

СОДЕРЖАНИЕ

Введение

В настоящее время информация является очень ценным ресурсом, поэтому необходимо обеспечить ее защиту от различных угроз. В первой части работы будут изучены принципы функционирования межсетевого экрана, определены задачи, которые он решает, рассмотрены различные способы его размещения и выявлены недостатки, связанные с его использованием.

Во второй части отчета будет проведен анализ различных документов, включающих требования к автоматизированным системам, вычислительной технике и информационным системам, обрабатывающим персональные данные. Кроме того, в этой части будет настроена подсистема регистрации и учета в домене на основе Windows Server 2003 с учетом требований безопасности, соответствующих необходимому уровню защищенности.

1 Межсетевые экраны

Далее будут рассмотрены понятие межсетевого экрана, основные виды межсетевых экранов и их классификация по способу размещения.

1.1 Понятие «Межсетевой Экран»

Межсетевой экран (англ. firewall) — это сетевое устройство или программное обеспечение, которое обеспечивает защиту компьютерных сетей от несанкционированного доступа и контролирует передачу данных между сетями с различными уровнями доверия. Он действует как фильтр, пропуская или блокируя сетевой трафик на основе заданных правил и политик безопасности.

Межсетевой экран может выполнять следующие функции:

- Фильтрация пакетов: Он проверяет каждый пакет данных, проходящий через него, и решает, разрешить или заблокировать его передачу на основе заданных правил фильтрации.
- Управление доступом: Межсетевой экран контролирует доступ к сетевым ресурсам, определяя, какие пользователи или устройства имеют право подключаться к определенным сервисам или портам.
- NAT и переадресация портов: Он может выполнять функции сетевого адресного перевода (NAT), позволяющего связывать внутренние локальные IP-адреса с общедоступными внешними IP-адресами, а также переадресацию портов для перенаправления запросов на определенные порты к определенным устройствам внутри сети.
- Виртуальная частная сеть (VPN): Некоторые межсетевые экраны поддерживают создание защищенных соединений VPN для безопасной передачи данных через общедоступные сети.
- Регистрация и журналирование событий: Межсетевой экран может записывать информацию о сетевой активности, а также событиях и инцидентах безопасности для последующего анализа.

Межсетевой экран является важным компонентом сетевой безопасности и используется для защиты сетей от широкого спектра угроз, включая

несанкционированный доступ, вредоносное программное обеспечение и атаки из интернета.

1.2 Основные типы МЭ и методы их работы

Межсетевые экраны можно разделить на два основных типа: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. Оба типа выполняют свои функции безопасности и способны блокировать запрещенный трафик, но их принципы работы отличаются. Правильная настройка обоих типов устройств позволяет достичь нужного уровня безопасности.

1.2.1 Межсетевые экраны прикладного уровня

Межсетевые экраны прикладного уровня, известные также как Application Layer Firewalls, представляют собой тип межсетевых экранов, которые работают на прикладном уровне модели OSI. Они обеспечивают более глубокий уровень анализа трафика, поскольку способны проанализировать содержимое передаваемых данных и применять правила безопасности, основанные на прикладных протоколах.

Межсетевые экраны данного типа осуществляют глубокий анализ трафика, включая содержимое пакетов и информацию о протоколах. Они позволяют контролировать доступ к приложениям и сервисам на основе прикладных правил, блокируя или разрешая доступ к конкретным веб-сайтам, почтовым серверам, файловым сервисам и другим приложениям. Кроме того, они предоставляют возможность создания детальных политик безопасности, основанных на характеристиках приложений, и могут выполнять проксирование и инспекцию содержимого, позволяя фильтровать и контролировать трафик на основе содержания данных.

Межсетевые экраны прикладного уровня также способны обеспечивать защиту от атак на приложения, обнаруживая подозрительную активность и предотвращая SQL-инъекции, кросс-сайтовые сценарии и другие типы атак на уровне приложений. Они также предоставляют возможность регистрировать и

мониторить события и активность сети на прикладном уровне, что позволяет анализировать сетевую активность и проводить аудит безопасности.

При использовании межсетевого экрана прикладного уровня, все соединения проходят через него. В начале соединение устанавливается на системе-клиенте и поступает на внутренний интерфейс межсетевого экрана. Затем, межсетевой экран принимает соединение и производит анализ содержимого пакета и используемого протокола. Он проверяет соответствие данного трафика правилам политики безопасности. Если соответствие обнаружено, межсетевой экран устанавливает новое соединение между своим внешним интерфейсом и системой-сервером.

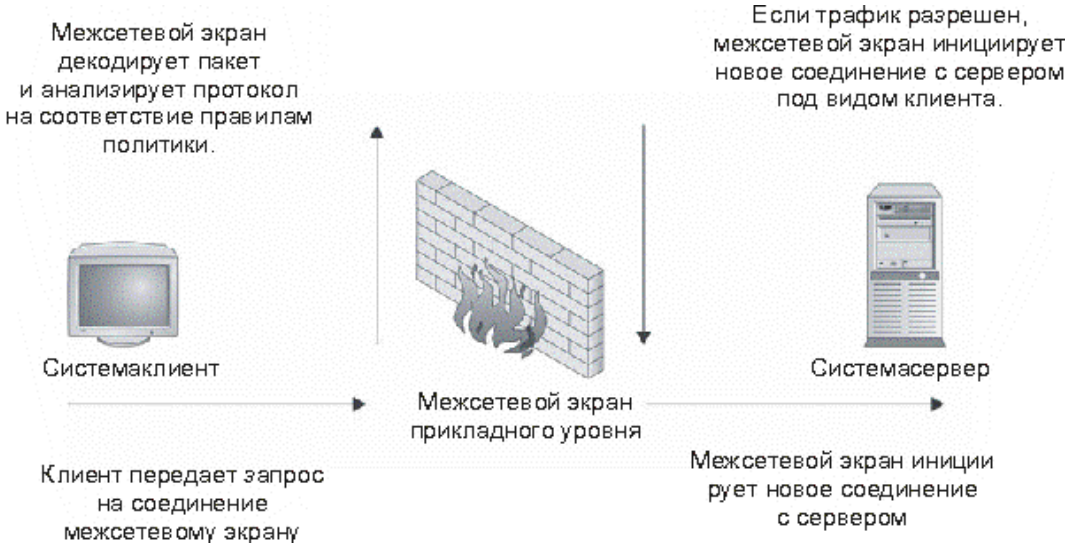

Рисунок 1 – Соединения модуля доступа межсетевого экрана прикладного уровня

Межсетевые экраны прикладного уровня используют модули доступа для обработки входящих подключений. Когда межсетевой экран получает входящее подключение, модуль доступа внутри него принимает его и обрабатывает команды, прежде чем отправить трафик получателю. Таким образом, межсетевой экран служит защитой системы от атак, которые могут быть осуществлены через приложения.

Обобщая вышесказанное, можно заключить, что межсетевые экраны прикладного уровня имеют более широкий набор функций и предназначены для более сложных сценариев безопасности и приложений, где требуется более тонкая настройка и контроль трафика на прикладном уровне.

1.2.2 Межсетевые экраны с пакетной фильтрацией

Межсетевые экраны с пакетной фильтрацией являются типом межсетевых экранов, которые базируются на фильтрации сетевых пакетов данных. Они работают на сетевом и транспортном уровнях модели OSI и выполняют несколько функций безопасности.

Основная функция межсетевых экранов с пакетной фильтрацией - фильтрация пакетов данных. Каждый сетевой пакет, проходящий через межсетевой экран, анализируется с помощью определенных правил и политик безопасности. Отправляющийся или получающийся пакет может быть разрешен или заблокирован в зависимости от параметров, таких как IP-адрес отправителя и получателя, порт, протокол и другие характеристики пакета.

Межсетевые экраны с пакетной фильтрацией также обеспечивают управление доступом. Они контролируют доступ к сетевым ресурсам, позволяя определить, какие устройства или пользователи имеют разрешение на доступ к конкретным сервисам или портам.

Кроме того, межсетевые экраны с пакетной фильтрацией поддерживают функции сетевого адресного перевода (NAT) и переадресацию портов. Это позволяет связывать внутренние локальные IP-адреса с внешними общедоступными IP-адресами и перенаправлять запросы на определенные порты к конкретным устройствам внутри сети.

Межсетевые экраны с пакетной фильтрацией обеспечивают базовую защиту от некоторых видов атак, включая атаки переполнения буфера и атаки с отказом в обслуживании (DoS). Однако они не обладают расширенными возможностями анализа содержимого пакетов, как межсетевые экраны прикладного уровня.

Основное преимущество межсетевых экранов с пакетной фильтрацией заключается в их простоте и эффективности. Они работают на сетевом уровне и способны обрабатывать сетевой трафик с высокой скоростью и низкой нагрузкой на ресурсы.

В целом, межсетевые экраны с пакетной фильтрацией представляют собой базовый уровень защиты сети, фокусирующийся на фильтрации пакетов данных и контроле доступа. Они широко используются для обеспечения безопасности в сетях и являются важным компонентом общей стратегии защиты информации.

При использовании межсетевого экрана с пакетной фильтрацией соединения не прерываются на самом экране, а направляются напрямую к конечной системе. При поступлении пакетов на межсетевой экран, он проводит проверку, разрешен ли данный пакет согласно правилам политики безопасности и состоянию соединения. Если пакет соответствует правилам, он передается по своему маршруту. В случае, если пакет не разрешен, он либо отклоняется, либо отменяется.

Рисунок 2 – Передача трафика через межсетевой экран с фильтрацией пакетов.

1.3 Принципы работы межсетевых экранов

Существует два основных подхода к созданию наборов правил межсетевого экрана: исключающий и включающий. Исключающий межсетевой экран разрешает проход всего трафика, за исключением трафика, который соответствует определенному набору правил. Включающий межсетевой экран, напротив, разрешает только трафик, соответствующий правилам, и блокирует все остальное.

Включающий межсетевой экран предоставляет более глубокий контроль над исходящим трафиком, что делает его предпочтительным выбором для

систем, предоставляющих услуги в Интернете. Он также контролирует типы трафика, генерируемого извне и направляемого в вашу частную сеть. Трафик, который не соответствует правилам, блокируется, и в журнале протоколируются соответствующие записи. Включающие межсетевые экраны обычно обеспечивают более высокий уровень безопасности по сравнению с исключающими, поскольку они снижают риск прохождения нежелательного трафика через межсетевой экран.

Дополнительный уровень безопасности может быть достигнут с помощью "межсетевого экрана с сохранением состояния". Такой межсетевой экран сохраняет информацию о активных соединениях и разрешает только трафик через открытые соединения или установку новых соединений. Недостатком межсетевого экрана с сохранением состояния является его уязвимость для атак типа DoS (отказ в обслуживании), особенно если большое количество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать функциональность с сохранением состояния и без сохранения состояния, что позволяет создавать оптимальные конфигурации для каждой конкретной системы.

1.4 Классификация по способу размещения

Для защиты корпоративной или локальной сети применяются следующие основные схемы организации межсетевых экранов

- Межсетевой экран, представленный как фильтрующий маршрутизатор
- Межсетевой экран на основе двухпортового шлюза
- Межсетевой экран на основе экранированного шлюза
- Межсетевой экран с экранированной подсетью

1.4.1 Межсетевой экран как фильтрующий маршрутизатор

Межсетевой экран, основанный на фильтрации пакетов, является наиболее распространенным и простым в реализации. Он представляет собой фильтрующий маршрутизатор, размещенный между защищаемой сетью и Интернетом.

Фильтрующий маршрутизатор настроен на блокирование или фильтрацию входящих и исходящих пакетов на основе анализа их адресов и портов. Компьютеры внутри защищаемой сети имеют прямой доступ в Интернет, но доступ к ним из Интернета ограничен. В основном, фильтрующий маршрутизатор может реализовать любую политику безопасности, которая была описана ранее.

Однако, если маршрутизатор не фильтрует пакеты на основе порта источника, входного и выходного портов, то реализация политики "все, что не разрешено, запрещено" может быть затруднена и требовать дополнительных настроек.

1.4.2 Межсетевой экран на основе двухпортового шлюза

Межсетевой экран на основе двухпортового прикладного шлюза представляет собой хост с двумя сетевыми интерфейсами, где осуществляется основная фильтрация информации между этими интерфейсами. Для дополнительной защиты между прикладным шлюзом и Интернетом устанавливается фильтрующий маршрутизатор. Это создает внутреннюю экранированную подсеть между шлюзом и маршрутизатором, которую можно использовать для размещения информационного сервера, доступного извне. Это повышает безопасность сети, поскольку даже при нарушении безопасности на информационном сервере злоумышленник не сможет получить доступ к системам сети через двухпортовый шлюз.

В отличие от схемы межсетевого экрана с фильтрующим маршрутизатором, прикладной шлюз полностью блокирует IP-трафик между Интернетом и защищаемой сетью. Только авторизованные приложения, установленные на прикладном шлюзе, могут предоставлять услуги и доступ пользователям.

Такая схема межсетевого экрана реализует политику безопасности, основанную на принципе "запрещено все, что не разрешено явно". Пользователям доступны только те службы, для которых определены соответствующие полномочия. Этот подход обеспечивает высокий уровень

безопасности, поскольку маршруты к защищенной подсети известны только межсетевому экрану и скрыты от внешних систем.

Эта схема межсетевого экрана относительно проста и эффективна. Поскольку используется хост, на межсетевом экране можно установить программы для усиленной аутентификации пользователей. Он также может вести протоколирование доступа, попыток зондирования и атак на систему, что позволяет выявить действия злоумышленников.

1.4.3 Межсетевой экран на основе экранированного шлюза

Межсетевой экран на основе экранированного шлюза обладает большей гибкостью по сравнению с межсетевым экраном, основанным на шлюзе с двумя интерфейсами. Однако, это сопряжено с некоторым уменьшением безопасности. В этой схеме межсетевой экран состоит из фильтрующего маршрутизатора и прикладного шлюза, размещенного со стороны внутренней сети. Прикладной шлюз является хостом и имеет только один сетевой интерфейс.

В данной конфигурации первичная безопасность обеспечивается фильтрующим маршрутизатором, который фильтрует или блокирует потенциально опасные протоколы, чтобы они не достигли прикладного шлюза и внутренних систем. Пакетная фильтрация в фильтрующем маршрутизаторе может быть настроена по следующим принципам:

- Разрешение внутренним хостам открывать соединения с хостами в сети Интернет для определенных сервисов, которые являются частью политики пакетной фильтрации.
- Запрет всех соединений от внутренних хостов, за исключением уполномоченных приложений на прикладном шлюзе.

В такой конфигурации межсетевой экран может использовать комбинацию двух политик в зависимости от политики безопасности, принятой внутри сети. Конкретно, пакетная фильтрация на фильтрующем маршрутизаторе может быть настроена таким образом, чтобы прикладной

шлюз, используя свои уполномоченные приложения, предоставлял сервисы типа Telnet, FTP, SMTP для систем внутри сети.

Основной недостаток схемы межсетевого экрана с экранированным шлюзом заключается в том, что если злоумышленник сможет проникнуть в хост, то системы внутренней сети останутся незащищенными. Еще одним недостатком является возможность компрометации маршрутизатора. Если маршрутизатор будет скомпрометирован, внутренняя сеть станет доступной для злоумышленника.

1.4.4 Межсетевой экран с экранированной подсетью

Межсетевой экран с экранированной подсетью является развитием схемы межсетевого экрана на основе экранированного шлюза. В этой схеме используются два экранирующих маршрутизатора, где внешний маршрутизатор размещается между Интернетом и экранируемой подсетью, а внутренний маршрутизатор - между экранируемой подсетью и защищаемой внутренней сетью. Экранируемая подсеть включает прикладной шлюз, а также информационные серверы и другие системы, требующие контролируемого доступа. Эта схема обеспечивает высокий уровень безопасности путем создания экранированной подсети, которая лучше изолирует внутреннюю защищаемую сеть от Интернета.

Внешний маршрутизатор служит для защиты экранированной подсети и внутренней сети от вторжений из Интернета. Он запрещает доступ извне к системам внутренней сети и блокирует весь трафик, идущий от систем, которые не должны инициировать соединения. Он также может блокировать другие уязвимые протоколы, которые не должны передаваться или поступать к хост-компьютерам внутренней сети.

Внутренний маршрутизатор обеспечивает защиту внутренней сети от несанкционированного доступа как из Интернета, так и из экранированной подсети. Он выполняет большую часть пакетной фильтрации и управляет трафиком к системам внутренней сети и от них.

Межсетевой экран с экранированной подсетью хорошо подходит для защиты сетей с большим объемом трафика или высокими скоростями передачи данных.

Недостатком этой схемы является необходимость уделять внимание конфигурации пары фильтрующих маршрутизаторов, чтобы обеспечить необходимый уровень безопасности, поскольку ошибки в их настройке могут привести к нарушению системы безопасности всей сети. Кроме того, существует возможность обхода прикладного шлюза в этой схеме.

1.5 Недостатки применения межсетевых экранов

Межсетевые экраны применяются для создания защищенных виртуальных частных сетей, объединяющих несколько локальных сетей, подключенных к глобальной сети. Передача данных между этими локальными сетями происходит незаметно для пользователей, и конфиденциальность и целостность информации обеспечиваются с помощью шифрования, цифровых подписей и других средств защиты. Для обеспечения безопасности могут быть зашифрованы не только данные внутри пакета, но и некоторые поля заголовка.

Однако межсетевые экраны имеют свои ограничения и не могут решить все проблемы безопасности корпоративных сетей. Некоторые из ограничений, связанных с применением межсетевых экранов, включают:

- Наличие уязвимых мест. Межсетевые экраны не могут защитить сеть от черных входов или уязвимостей, существующих в самой сети. Например, если существует неограниченный доступ к сети через модем, межсетевой экран может быть обойден злоумышленниками.
- Недостаточная защита от внутренних угроз. Межсетевые экраны обычно не предоставляют защиту от вредоносных действий со стороны сотрудников компании или внутренних угроз.
- Ограничения в доступе к сервисам. Межсетевые экраны могут блокировать определенные сервисы, которые могут быть необходимы для работы пользователей, такие как Telnet или FTP. В таких случаях

требуется баланс между требованиями безопасности и потребностями пользователей.

- Концентрация средств безопасности в одном месте. Межсетевой экран позволяет сосредоточить средства обеспечения безопасности в одном месте, что упрощает его администрирование.
- Ограниченная пропускная способность. Межсетевые экраны могут ограничивать пропускную способность сети в зависимости от их возможностей и конфигурации.

2 Разработка и реализация требований для защиты подсистемы регистрации и учета

В данной работе рассматривается настройка подсистемы регистрации и учета в домене на базе Windows Server 2003 с учетом требований безопасности, предъявляемых к ИС, согласно требуемому уровню защищенности.

Рассмотрим предоставленную для выполнения задания систему:

- Организация: Дизайнерская фирма;
- Количество сотрудников: 30;
- Подразделения: Главный менеджер, отделы: кадров, бухгалтерия, кухонного дизайна, ландшафтного дизайна;
- Количество обслуживаемых клиентов: 1000;
- Вид конфиденциальной информации или ПДн: Пдн (сотрудники, общедоступные, специальные);
- Наличие удаленного доступа (абонент за пределами КЗ): Нет.
- При настройке подсистемы учета и регистрации в домене будем учитывать следующие параметры:
- В каждом отделе имеются как минимум два рядовых сотрудника и один начальник отдела;
- Все сотрудники имеют одинаковые права в рамках своего отдела;
- У каждого сотрудника имеется свой личный каталог на сервере, кроме того, для всех сотрудников предоставляется один общий каталог для обмена данными внутри отдела;
- Начальник отдела имеет доступ к каталогам и файлам сотрудников в рамках проверки, но не имеет права вносить в них какие-либо изменения без ведома сотрудников.

2.1 Определение требуемого уровня защищенности

Согласно руководящему документу «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и

требования по защите информации» (далее – РД АС) определим требуемый уровень защищенности АС.

В информационной системе организации хранятся и обрабатываются данные разного уровня конфиденциальности (ПДн сотрудников и специальные Пдн). Исходя из этого можно заключиться что система относится к первой группе защищенности (согласно пункту 1.9 РД АС: «Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А» [7]).

Согласно пункту 5.2.3 руководящего документа «Специальные требования и рекомендации по технической защите конфиденциальной информации», (далее – СТР-К): «…устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального характера:

- АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;
- АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д [8].

Так как в данной информационной системе обрабатываются специальные ПДн, то ее можно отнести к классу 1Г.

В соответствии с РД АС и Руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 30.03.1992 (далее – РД СВТ), статья 1, пункт 1.4, устанавливается 5 класс защищенности СВТ [9].

В соответствии с Федеральным законом №149-ФЗ (ред. от 06.04.2011) «Об информации, информационных технологиях и защите информации» от 27.07.2006, статья 14, пункт 1, рассматриваемая система не является

государственной информационной системой. Поэтому необходимо рассмотреть Приказ ФСТЭК России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [10].

Для определения уровня защищенности ПДн определим актуальные типы угроз для данной информационной системы:

- Угрозы 1-го типа исключаются (в данной системе используется лицензионное системное ПО);
- Угрозы 2-го типа исключаются (инструментальное ПО, используемое в системе, является сертифицированным);
- Угрозы 3-го типа являются актуальными (угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе).

В соответствии с Постановлением Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 (ПП РФ №1119), пункт 11 (в):

«Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

в) Для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора» [11].

Таким образом следует установить 3-ий уровень защищенности персональных данных.

2.2 Определение защищаемых свойств информации

В рассматриваемой ИС обрабатываются ПДн, для их защиты необходимо обеспечить целостность, доступность и конфиденциальность.

2.3 Определение необходимых требований к системе

Для защиты от НСД АС класса 1Г, согласно РД АС, статья 2, пункт 2.12, должны осуществляться регистрация и учет следующих событий:

- регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова;
- регистрация выдачи печатных (графических) документов на «твердую» копию; • регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрация попыток доступа программных средств к терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;
- учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.
- Для защиты от НСД СВТ 5 класса согласно РД СВТ, пункт 2.3.5, должны осуществляться регистрация и учет следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для защиты от НСД согласно Приложению к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах 20 персональных данных Приказа № 21 ФСТЭК должны устанавливаться следующие требования для подсистемы регистрации и учета:

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности.

Для защиты от НСД ПДн уровня 3 согласно пунктам 13 и 14 ПП №1119 устанавливаются следующие требования к системе:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
- необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе

2.4 Реализация на виртуальных машинах системы клиент-сервер

Реализуем виртуальную машину, на которую установим ОС Windows Server 2003. Информация о созданном сервере показана на рисунке 3.

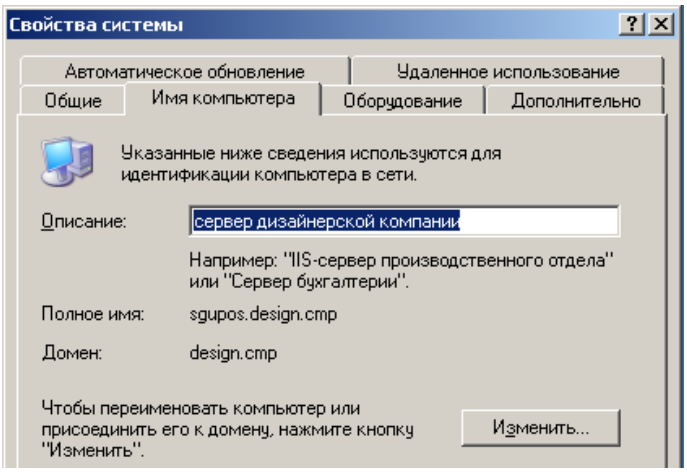

Рисунок 3 – Информация о сервере.

Создадим еще одну виртуальную машину-клиент, на которую установим Windows XP, и добавим данную машину-клиент в домен. Укажем имя домена и введем пароль администратора домена. На рисунке 4 продемонстрирована информация о машине-клиенте.

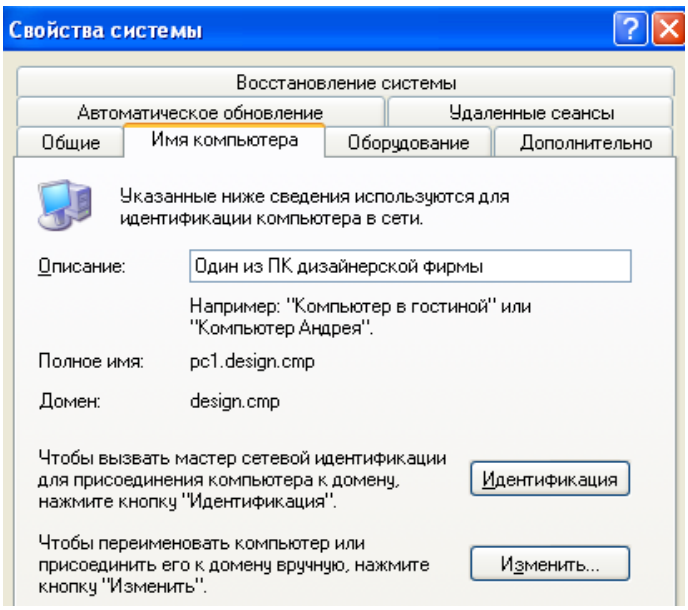

Рисунок 4 – Информация о клиенте.

Для выполнения задания необходимо создать организацию. Для этого на сервере воспользуемся оснасткой «Active Directory – пользователи и компьютеры» и создадим подразделение «Дизайнерская фирма». В нем создадим 5 подразделений – для каждого отдела организации и генерального менеджера. Результат показан на рисунке 5.

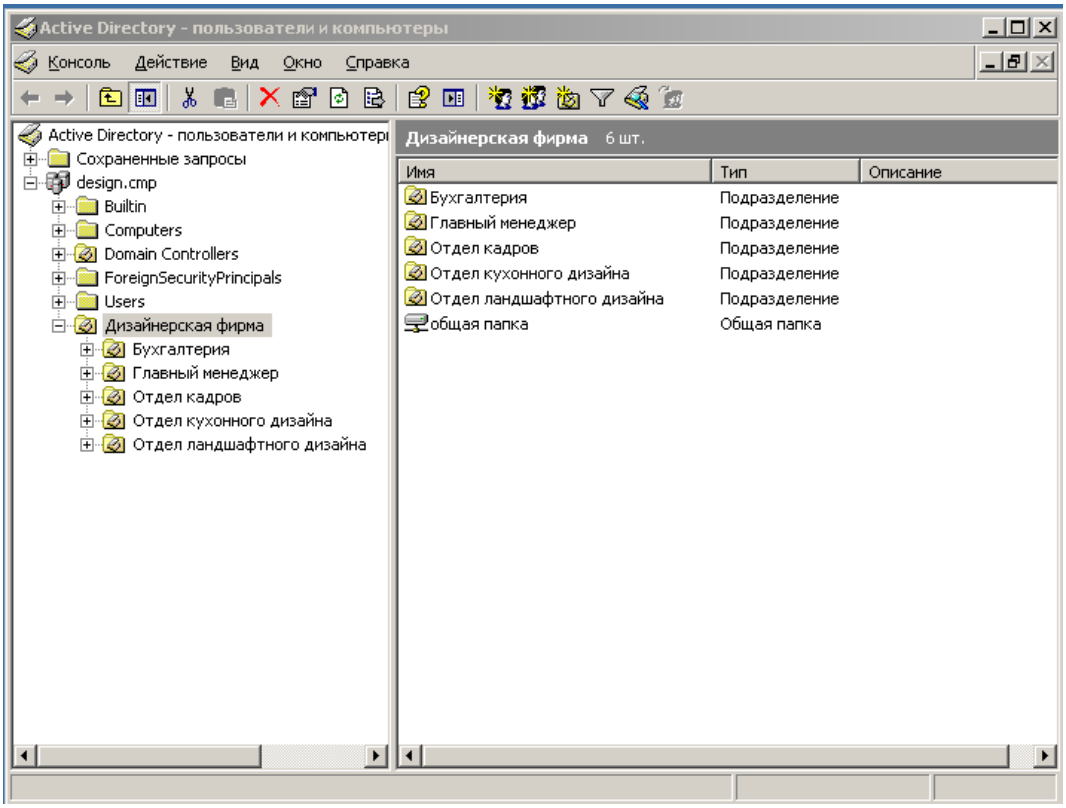

Рисунок 5 – Созданная организация.

Для демонстрации работы системы допустим, что помимо директора организации в каждом отделе числится три человека: начальник отдела и два сотрудника. У каждого сотрудника организации есть своя папка, папка подразделения и общая папка, к которой имеют полный доступ все сотрудники. Содержимое папки «Дизайнерская фирма», в которой размещены все остальные представлено на рисунке 6.

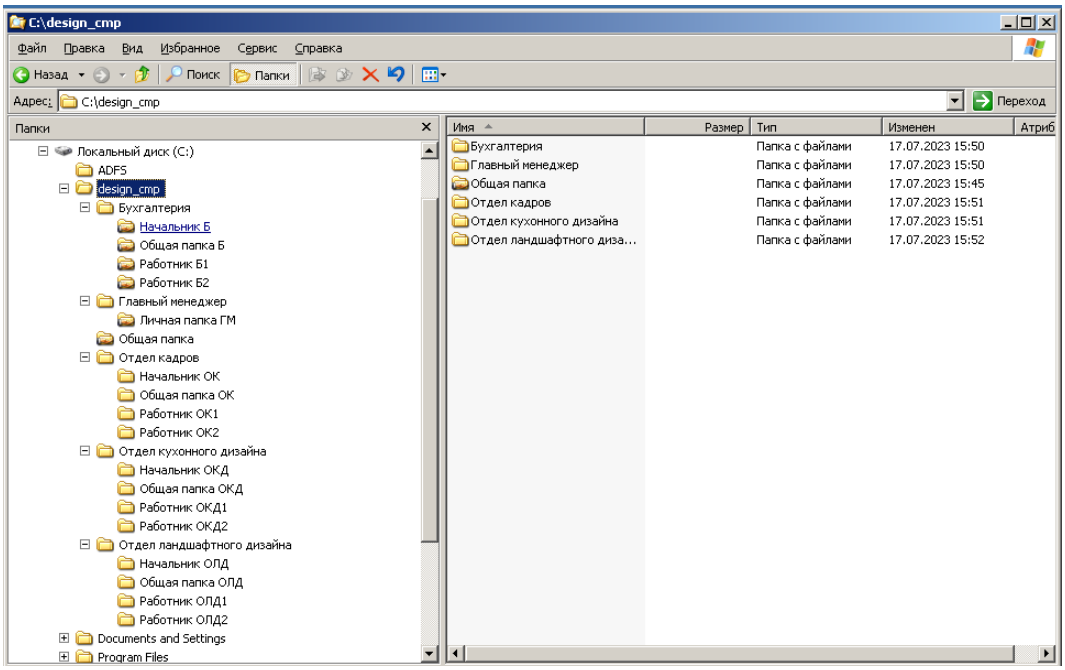

Рисунок 6 – Директории фирмы.

Матрица доступа в организации представлена в таблице (Рисунок 7). По горизонтали размещены роли сотрудников в организации, по вертикали – соответственно директории и содержащиеся в них файлы на сервере, к которым определяется доступ. Имеются 4 основных типа операций (атомы c, r, u и d), на которые выдаются разрешения конкретному сотруднику:

c – операция чтения;

r – операция записи;

u – операция модификации;

d – операция удаления.

В случае, когда необходимы несколько разрешений, несколько атомов складываются в слово (например слово crud обозначает доступ ко всем перечисленным операциям, а слово r – только к операции чтения).

			Роль в организации												
				ОК			ОКД			ОЛД			Б		
			ГМ	Н	Р1	Р2	Н	Р1	Р2	Н	Р1	Р2	Н	Р1	Р2
Директория		ГМ	crud	r	-	-	r	-	-	r	-	-	r	-	-
	ОК	Н	r	crud	-	-	-	-	-	-	-	-	-	-	-
		Р1	-	r	crud	-	-	-	-	-	-	-	-	-	-
		Р2	-	r	-	crud	-	-	-	-	-	-	-	-	-
		ОП	-	crud	crud	crud	-	-	-	-	-	-	-	-	-
	ОКД	Н	r	-	-	-	crud	-	-	-	-	-	-	-	-
		Р1	-	-	-	-	r	crud	-	-	-	-	-	-	-
		Р2	-	-	-	-	r	-	crud	-	-	-	-	-	-
		ОП	-	-	-	-	crud	crud	crud	-	-	-	-	-	-
	ОЛД	Н	r	-	-	-	-	-	-	-	-	-	-	-	-
		Р1	-	-	-	-	-	-	-	r	crud	-	-	-	-
		Р2	-	-	-	-	-	-	-	r	-	crud	-	-	-
		ОП	-	-	-	-	-	-	-	crud	crud	crud	-	-	-
	Б	Н	r	-	-	-	-	-	-	-	-	-	crud	-	-
		Р1	-	-	-	-	-	-	-	-	-	-	r	crud	-
		Р2	-	-	-	-	-	-	-	-	-	-	r	-	crud
		ОП	-	-	-	-	-	-	-	-	-	-	crud	crud	crud
	ОПВО		crud	crud	crud	crud	crud	crud	crud	crud	crud	crud	crud	crud	crud

Рисунок 7 - Матрица доступа

Список сокращений в матрице доступа:

ГМ – генеральный менеджер;

Н – начальник отдела;

Р1 и Р2 – работники (сотрудники) отдела;

ОК – отдел кадров;

ОКД – отдел кухонного дизайна;

ОЛД – отдел ландшафтного дизайна;

Б – бухгалтерия;

ОП – общая папка (конкретного отдела);

ОПВО – общая папка (для всех отделов).

Проверим правильность работы настроек доступа. Например, при попытке начальника отдела кадров зайти в папку генерального менеджера появляется уведомление «Отказано в доступе» (Рисунок 8).

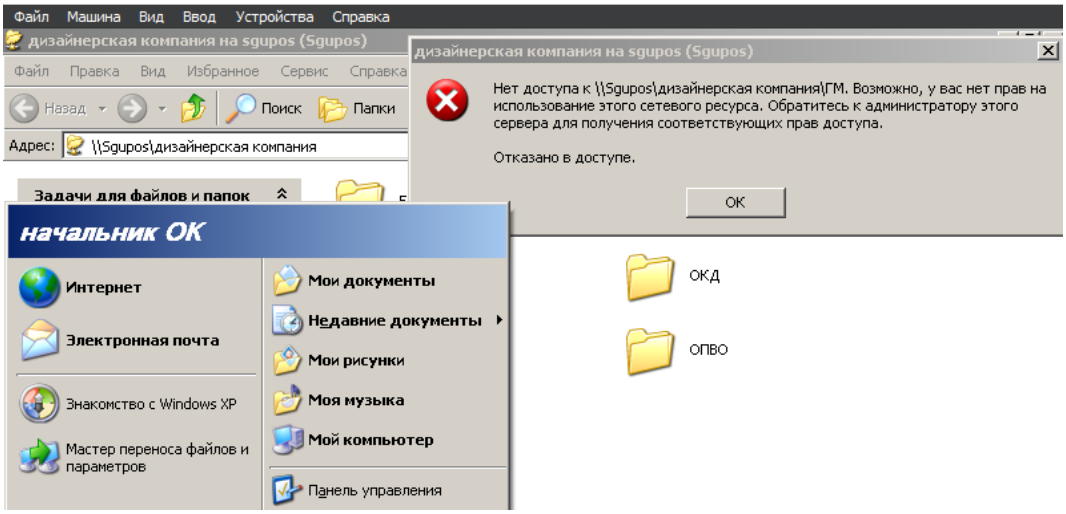

Рисунок 8 – Попытка начальника отдела зайти в папку генерального менеджера.

При этом начальник отдела кадров имеет доступ в собственную папку (Рисунок 9) и в папку одного из работников его отдела (Рисунок 10).

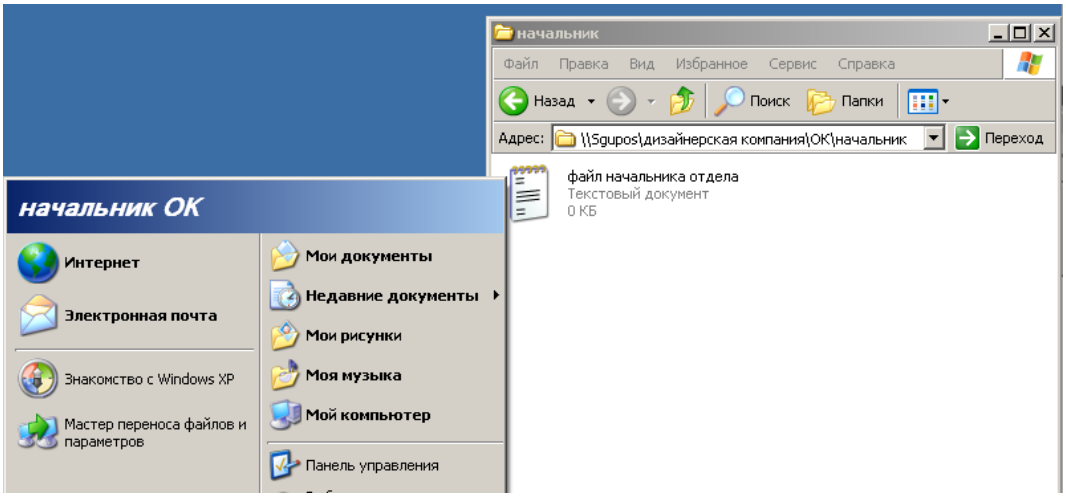

Рисунок 9 – Попытка начальника отдела зайти в свою папку.

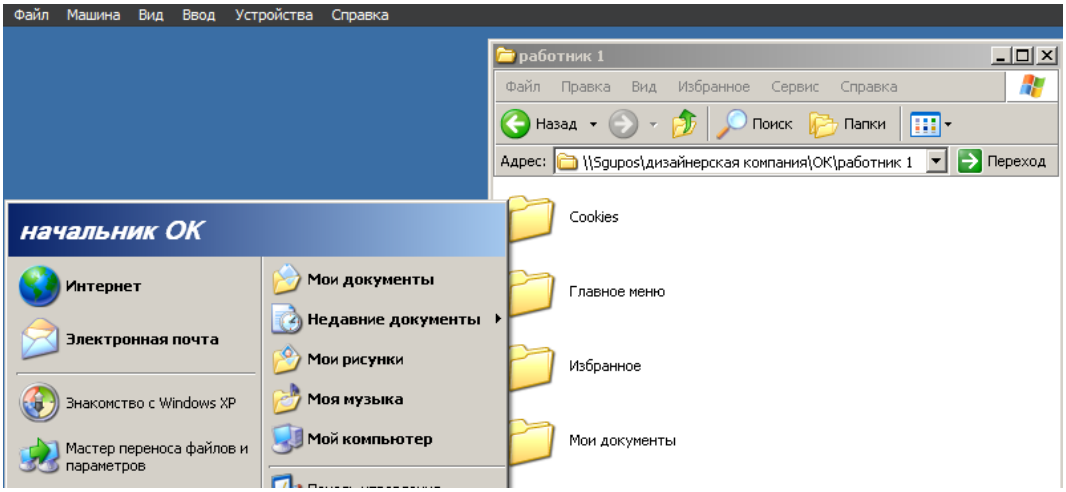

Рисунок 10 – Попытка начальника отдела зайти в папку сотрудника.

Однако, начальник отдела не может вносить какие-либо измения в файлы своих подчиненных. На рисунке 11 продемонстрированна попытка начальника отдела создать файл в папке работника отдела.

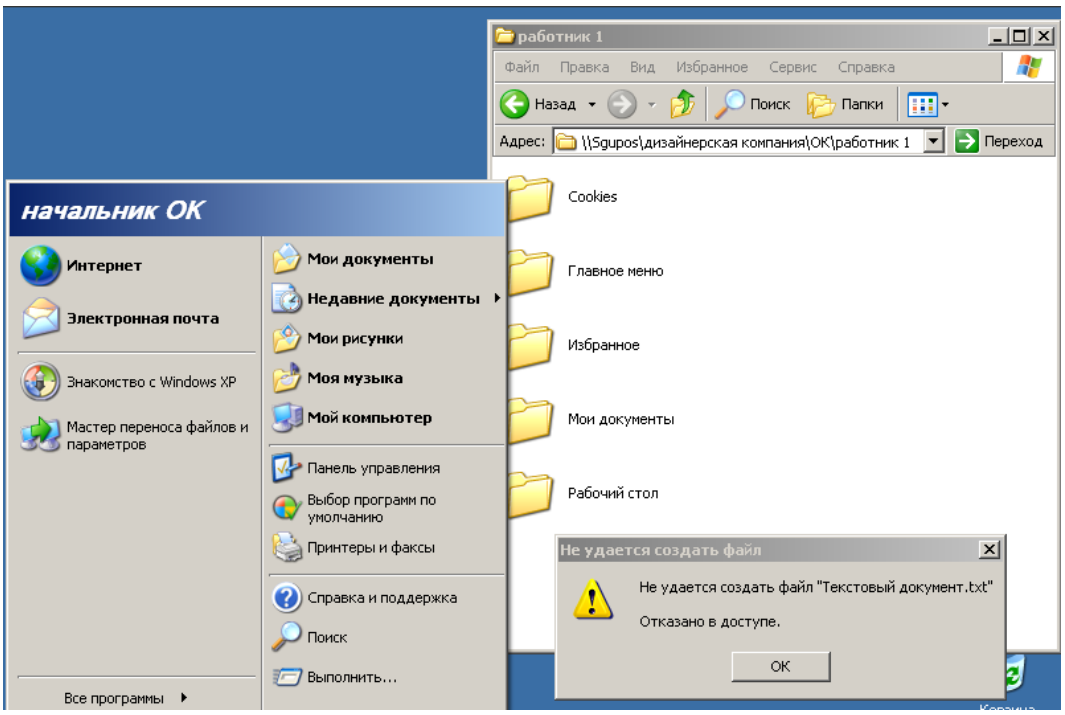

Рисунок 11 – попытка начальника отдела создать файл в папке работника отдела.

Кроме того, необходимо проверить возможность начальника отдела редактировать файлы своих подчиненных. Под учетной записью работника отдела кадров создадим текстовый файл «Текстовый документ.txt» и попробуем изменить его под учетной записью начальника этого отдела. Результат показан на рисунке 12.

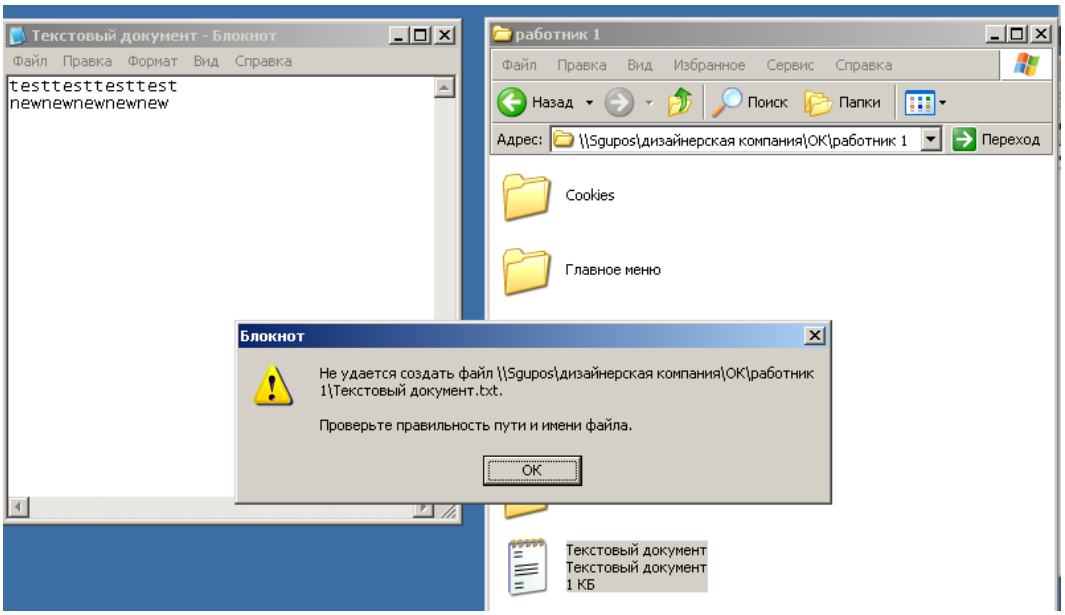

Рисунок 12 – Попытка начальника отдела редактировать файл сотрудника.

Важной частью системы является отсутствие доступа работников к личным папкам других работников того же отдела. Попытка сотрудника войти в папку другого сотрудника того же отдела показана на рисунке 13.

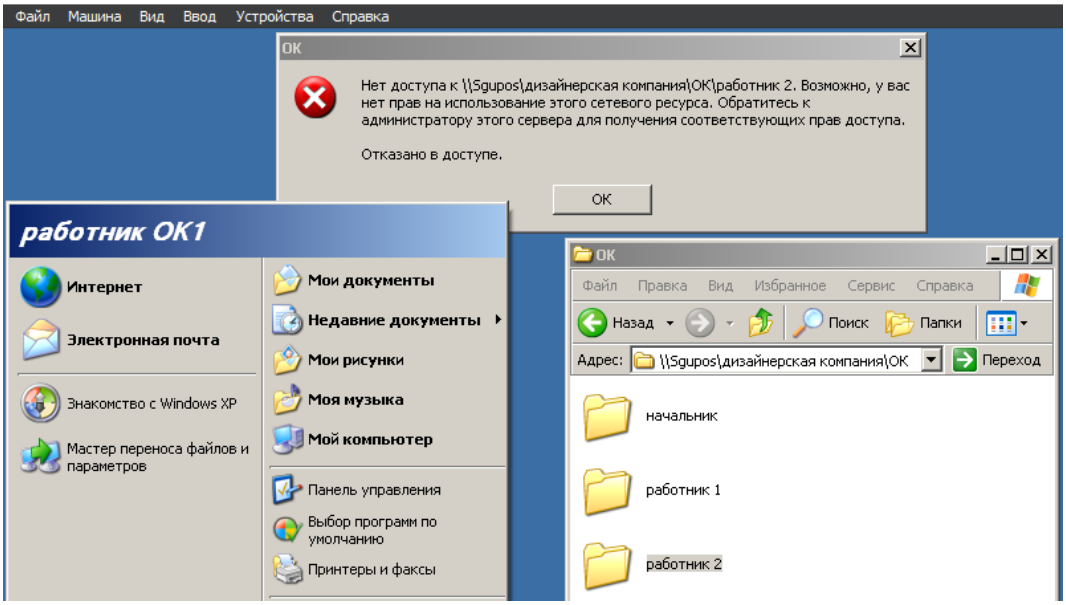

Рисунок 13 – Попытка одного сотрудника зайти в папку другого сотрудника

Аналогично, все сотрудники одного отдела не имеют доступа к папкам сотрудников других отделов.

2.5 Настройка подсистемы регистрации и учета

Реализуем требования к подсистеме регистрации и учета, согласно РД АС.

1. Вход (выход) субъектов доступа в (из) систему (Рисунки 14-16):

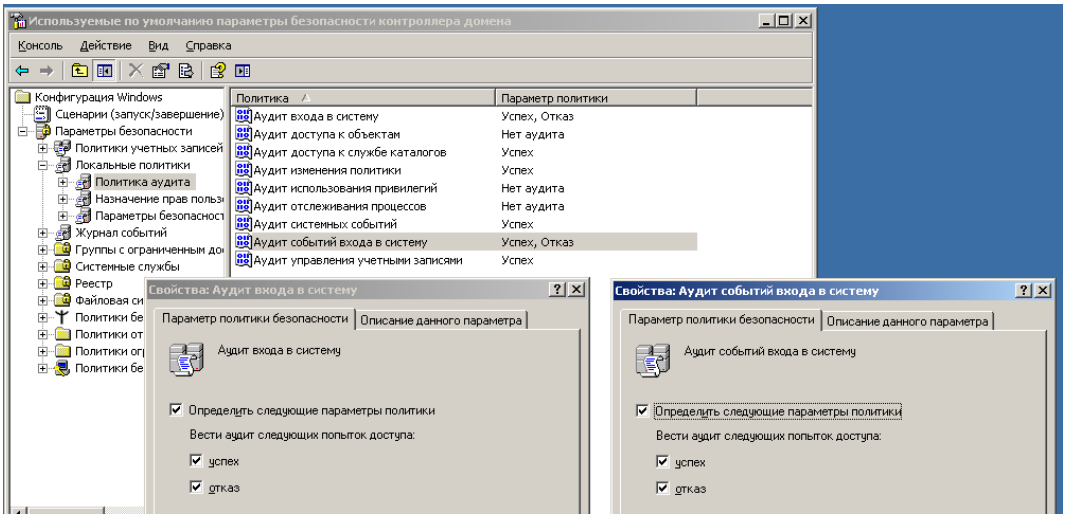

Рисунок 14 – Включение аудита событий входа (выхода) в систему.

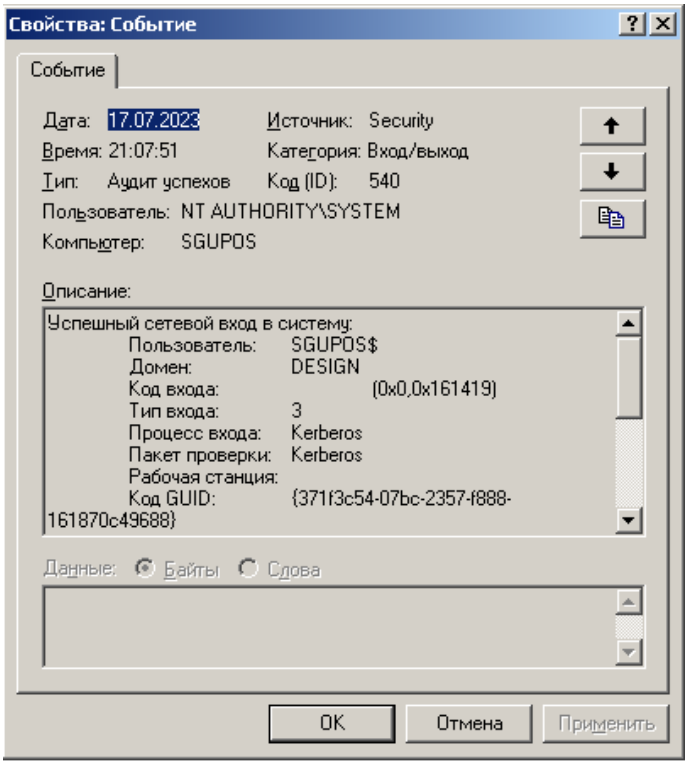

Рисунок 15 – Аудит успешного входа в систему.

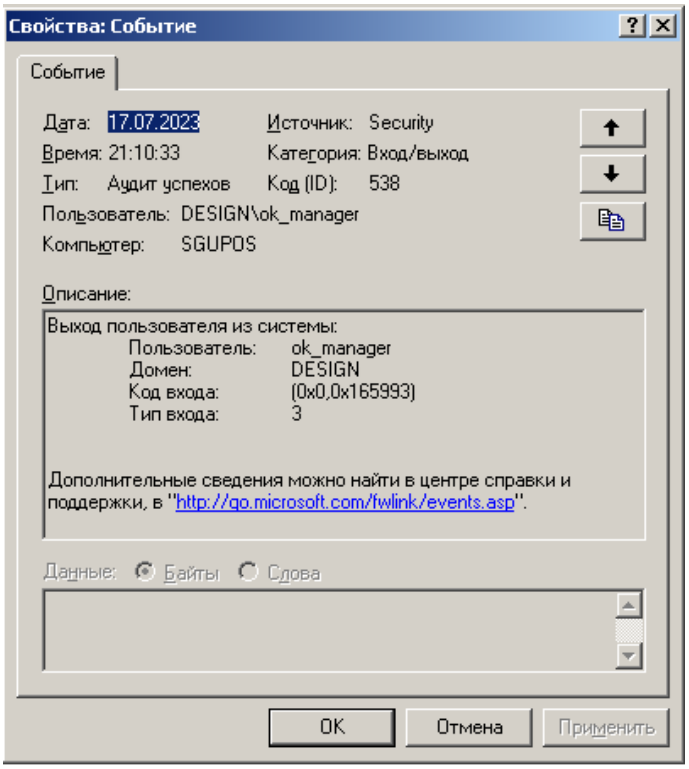

Рисунок 16 – Аудит успешного выхода в системы.

2. Выдача печатных выходных документов

   Запретим добавление и удаление принтеров (Рисунок 17).

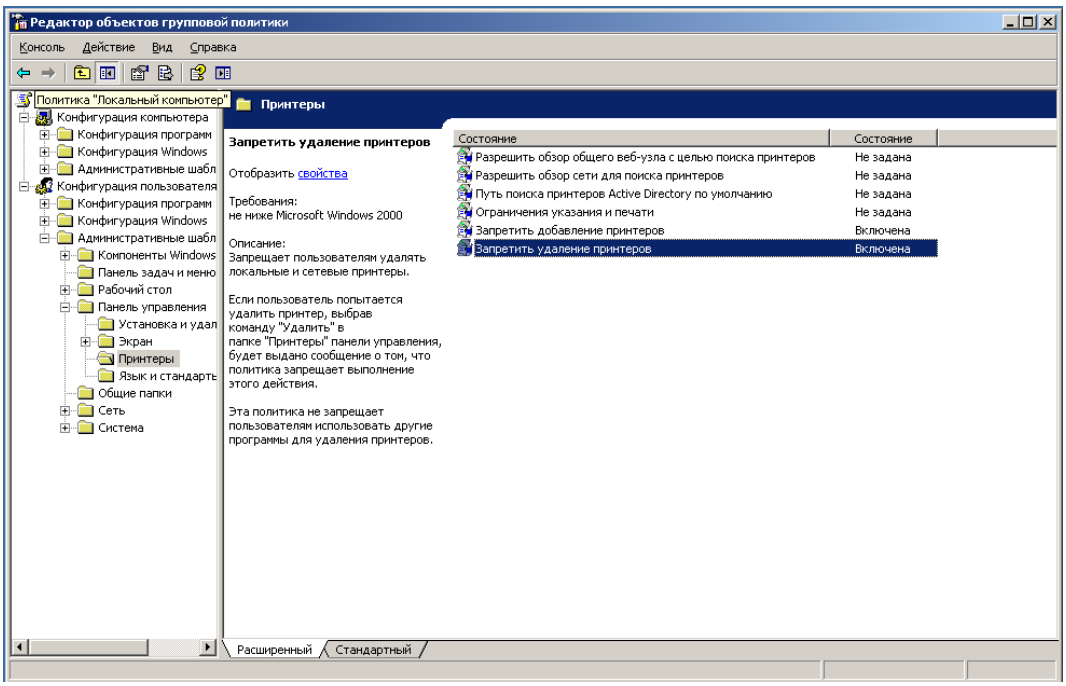

Рисунок 17 – Настройки для запрета установки и удаления принтеров.

Настроим аудит для всех сотрудников компании, которые могут осуществлять печать с принтера (Рисунок 18).

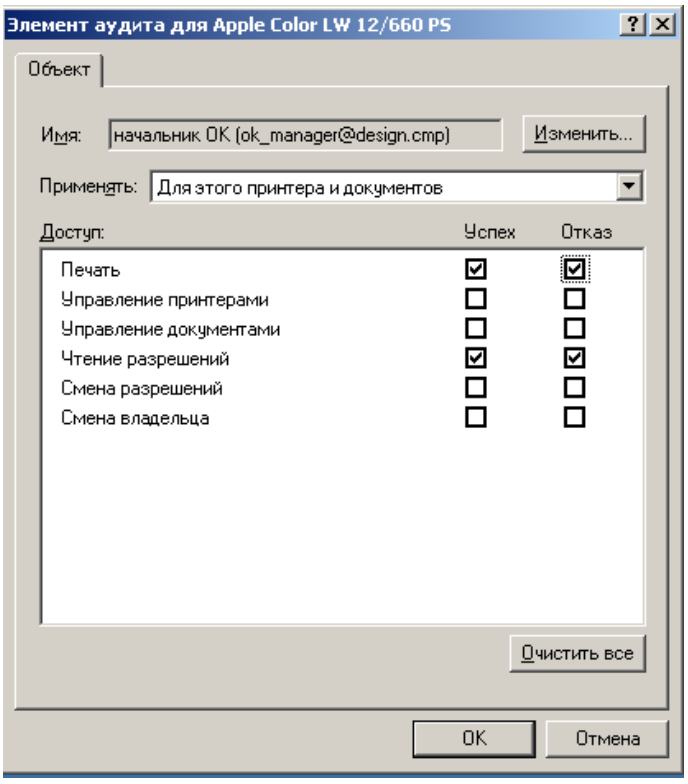

Рисунок 18 – Настройка аудита для принтера.

3. Запуск (завершение) программ и процессов

Включим аудит отслеживания процессов (Рисунок 19). Результат представлен на рисунках 20-21.

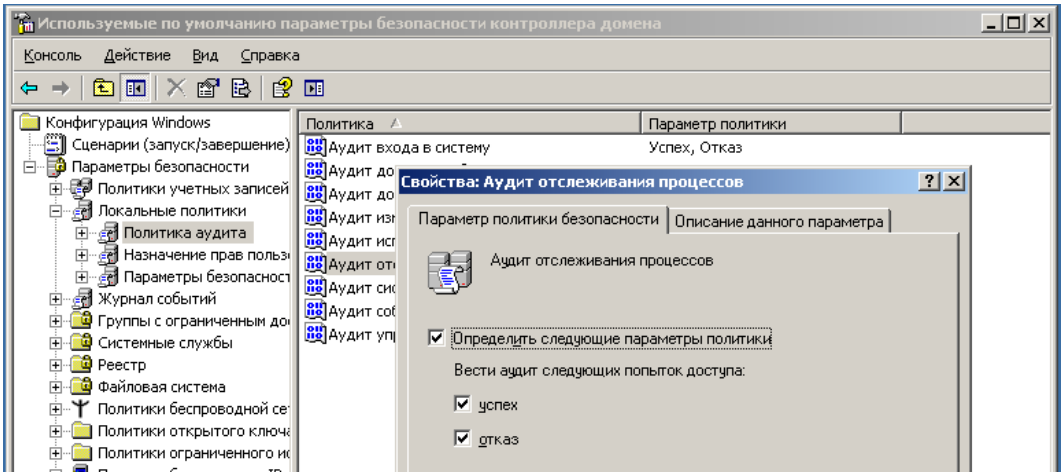

Рисунок 19 – Настройка аудита отслеживания процессов.

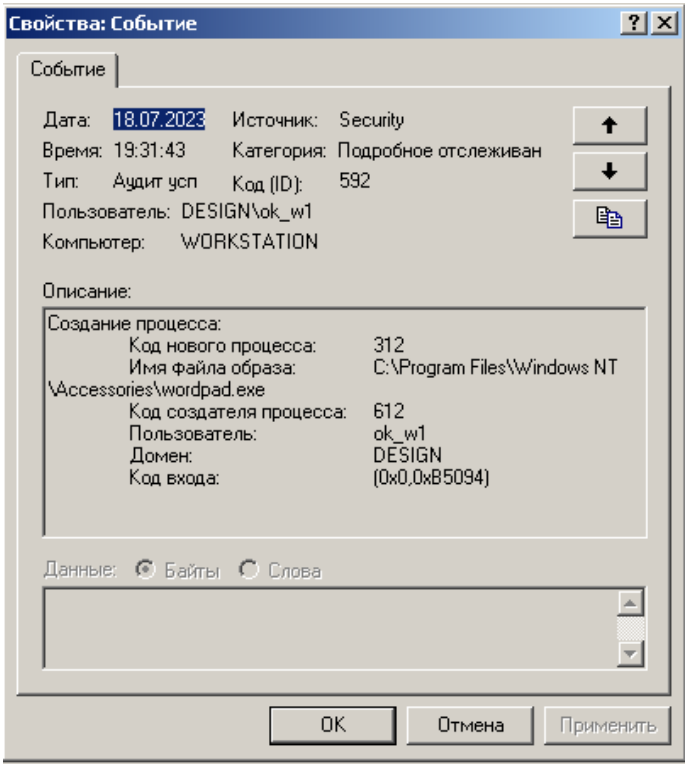

Рисунок 20 – Аудит успешного создания процесса.

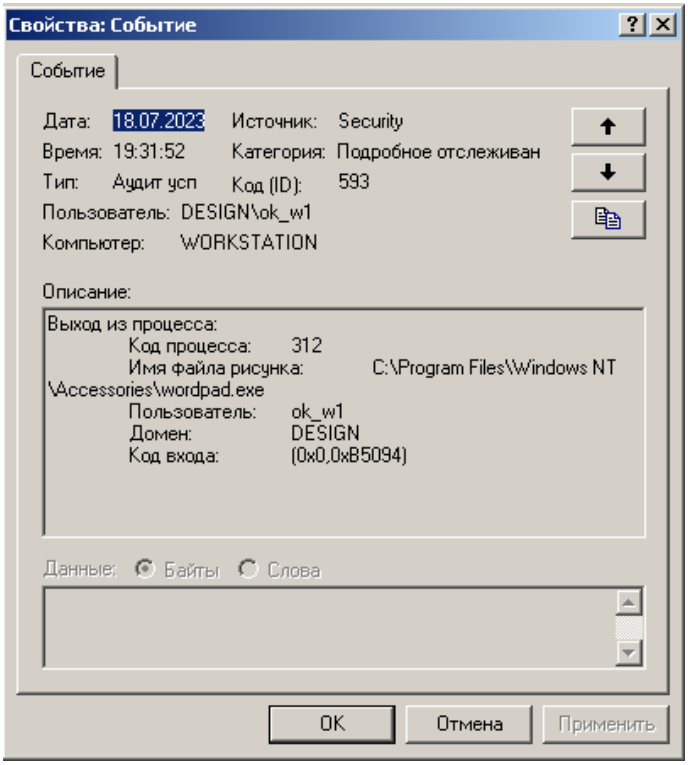

Рисунок 21 – Аудит успешного завершения процесса

4. Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам

Создадим пользователем «Работник ОК 1» текстовый файл в общем каталоге отдела кадров. При открытии файла, данная попытка регистрируется в журнале, причем с указанием полного пути к данному файлу, данный факт продемонстрирован на рисунке 22.

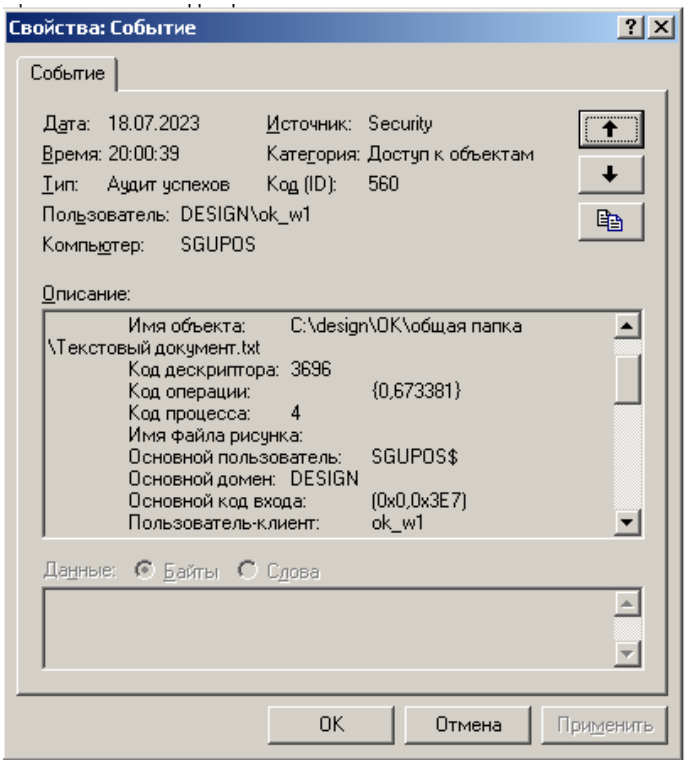

Рисунок 22 – Аудит успешного доступа к файлу.

Далее попробуем от пользователя «Начальник ОК» получить доступ к этому файлу через приложение «Блокнот». Как можно видеть на рисунке 23, был получен отказ доступа.

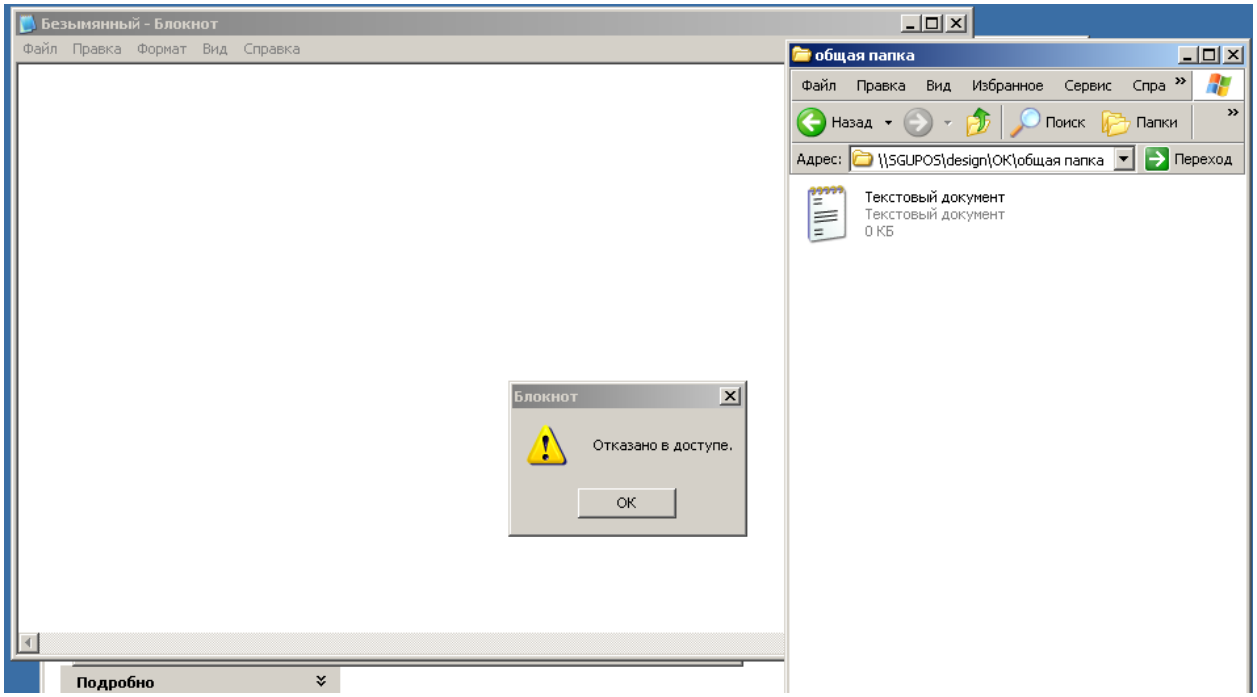

Рисунок 23 – Попытка открытия каталога через Notepad.

Данная попытка доступа была внесена в журнал безопасности. На рисунке 24 показан аудит отказа доступа к объектам

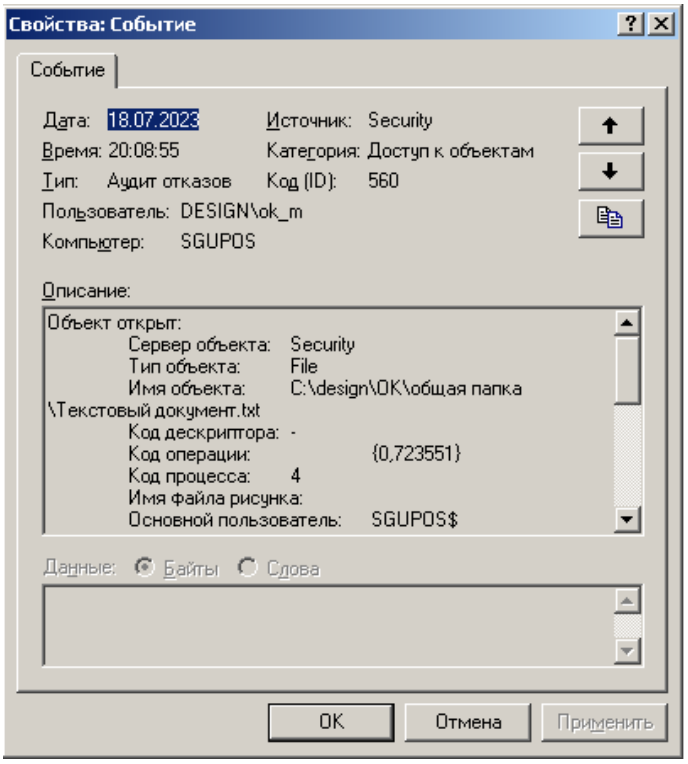

Рисунок 24 – Аудит отказа доступа к файлу.

5. Учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку) Обеспечивается организационными мерами.
6. Учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема) Обеспечивается организационными мерами.
7. Очистка освобождаемых областей оперативной памяти ЭВМ и внешних накопителей

Для настройки данного требования следует перейдем во вкладку «Параметры безопасности» и включим параметр «Очистка страничного файла», как показано на рисунке 25. При завершении работы будет произведена очистка оперативной памяти.

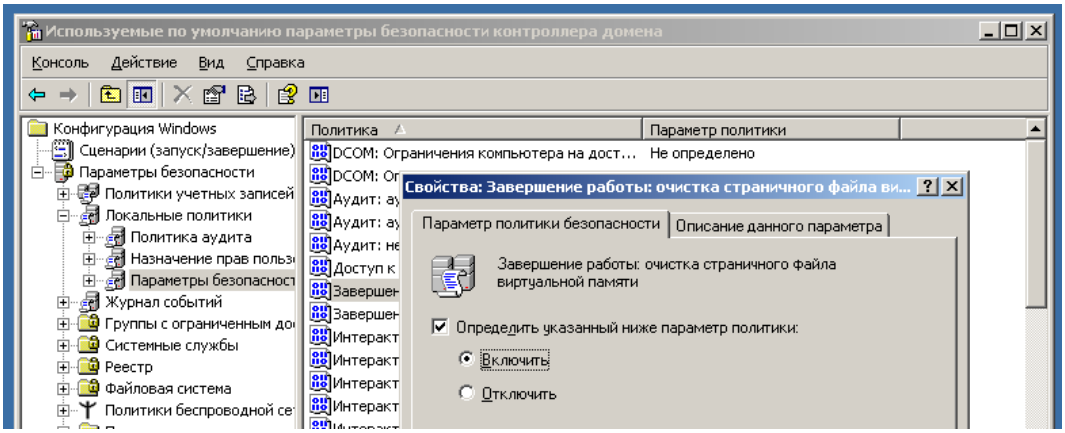

Рисунок 25 – Настройка очистки оперативной памяти.

Реализуем требования к подсистеме регистрации и учета согласно РД СВТ.

1. Использование идентификационного и аутентификационного механизма

   Реализовано согласно РД АС.

2. Запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)

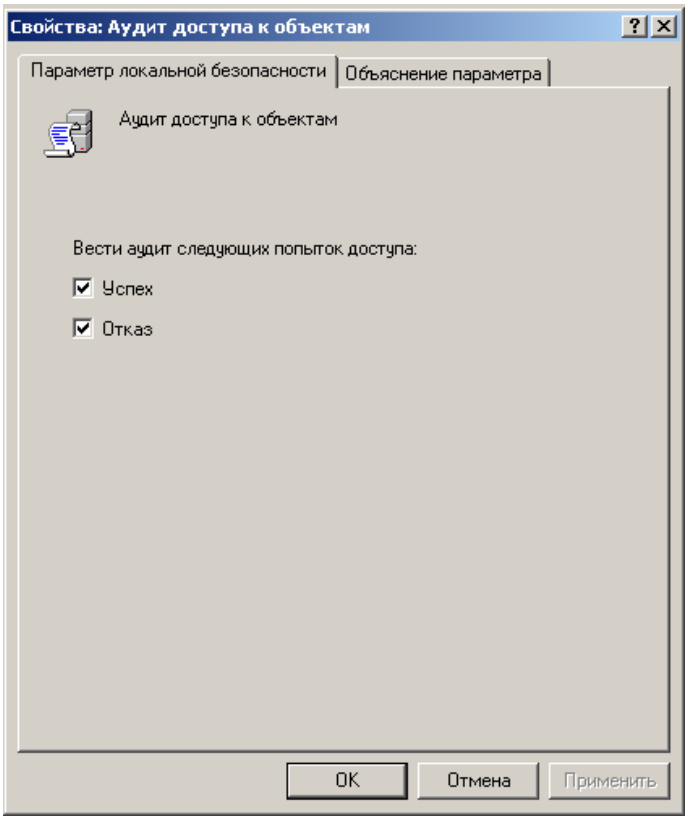

Рисунок 26 – Настройка аудита доступа к объектам.

Осуществим пользователем «Работник ОК 1» попытку доступа к двум объектам: файл в общей папке отдела кадров (Рисунок 27) и к каталогу отдела кадров (Рисунок 28).

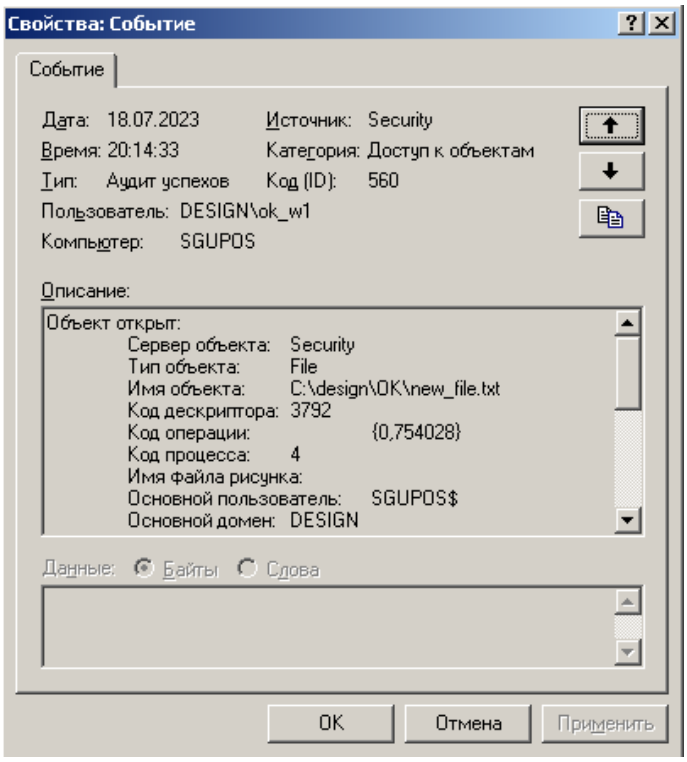

Рисунок 27 – Аудит успехов доступа к объектам.

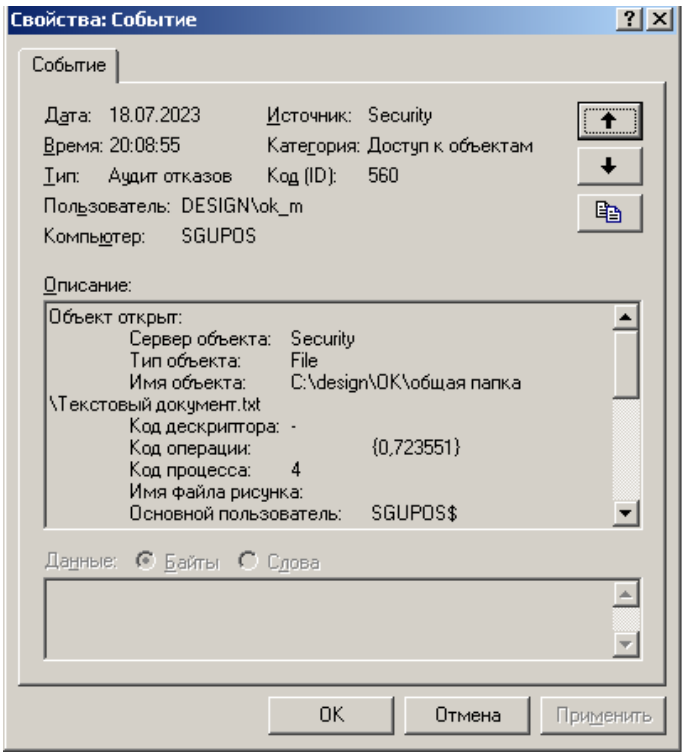

Рисунок 28 – Аудит отказов доступа к объектам.

3. Создание и уничтожение объекта

Для каждого пользователя необходимо настроить аудит успехов и отказов на создание и удаление файлов и каталогов, как показано на рисунке 29.

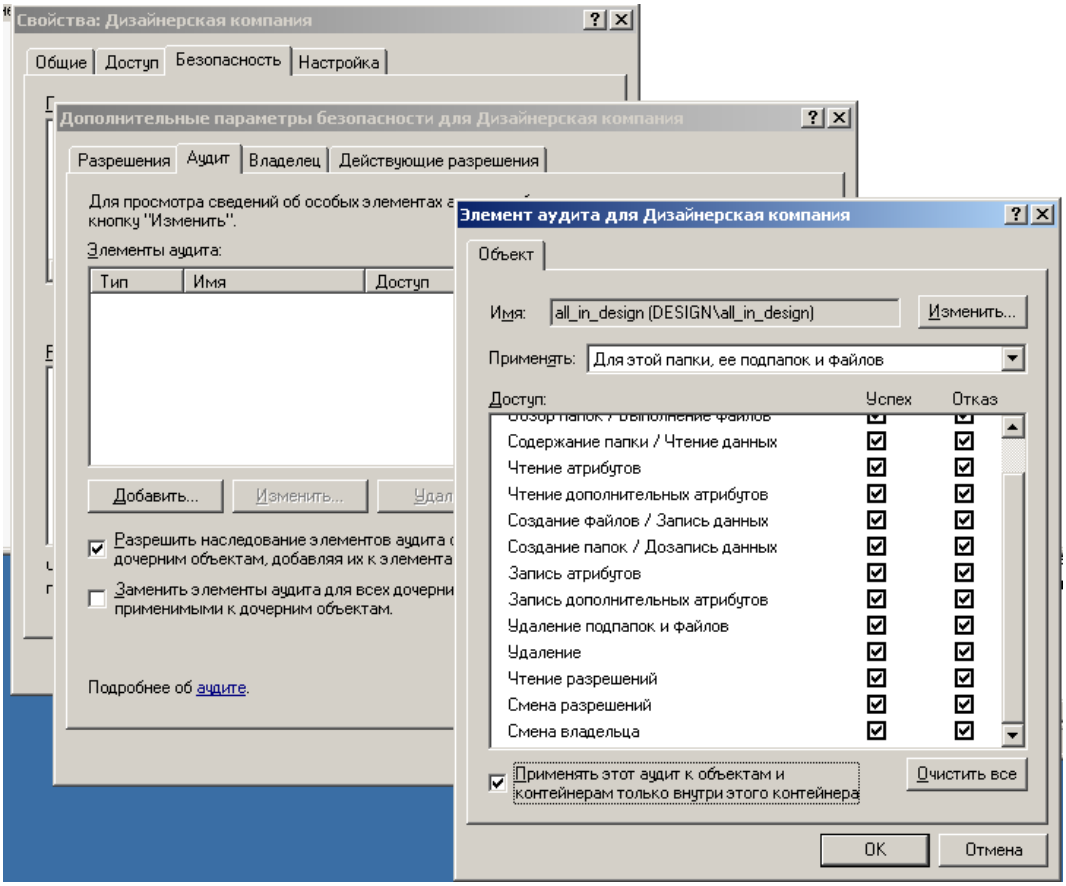

Рисунок 29 – Настройка аудита создания и уничтожения объекта.

На рисунке 30 показана запись в журнале событий при создании пользователем «Работник ОК 2» объекта в каталоге «Общая папка» отдела кадров. Удаление файла происходит аналогично.

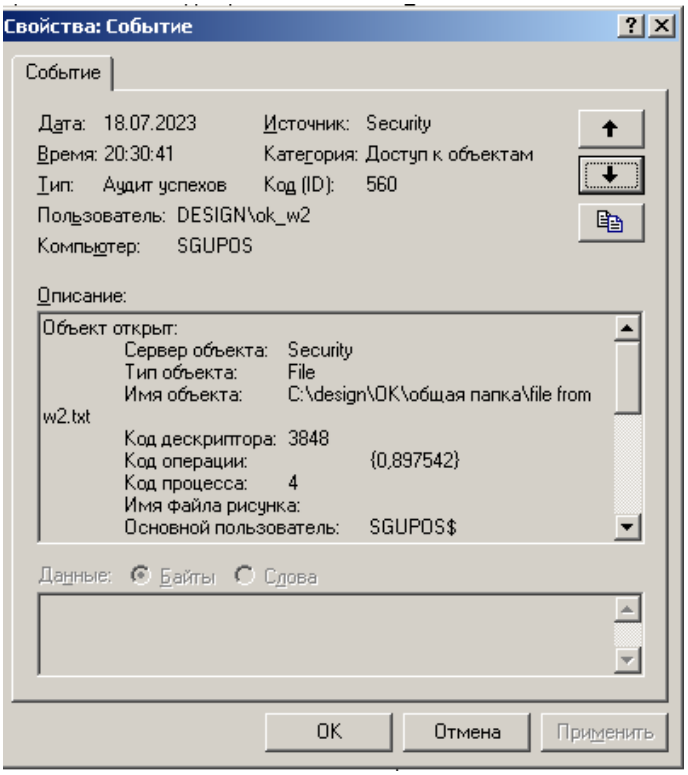

Рисунок 30 – Аудит успеха создания объекта.

Теперь попробуем создать объект в папке «Работник ОК 1» от пользователя «Начальник ОК», который имеет право только на чтение данной папки. Попытка создания представлена на рисунке 31.

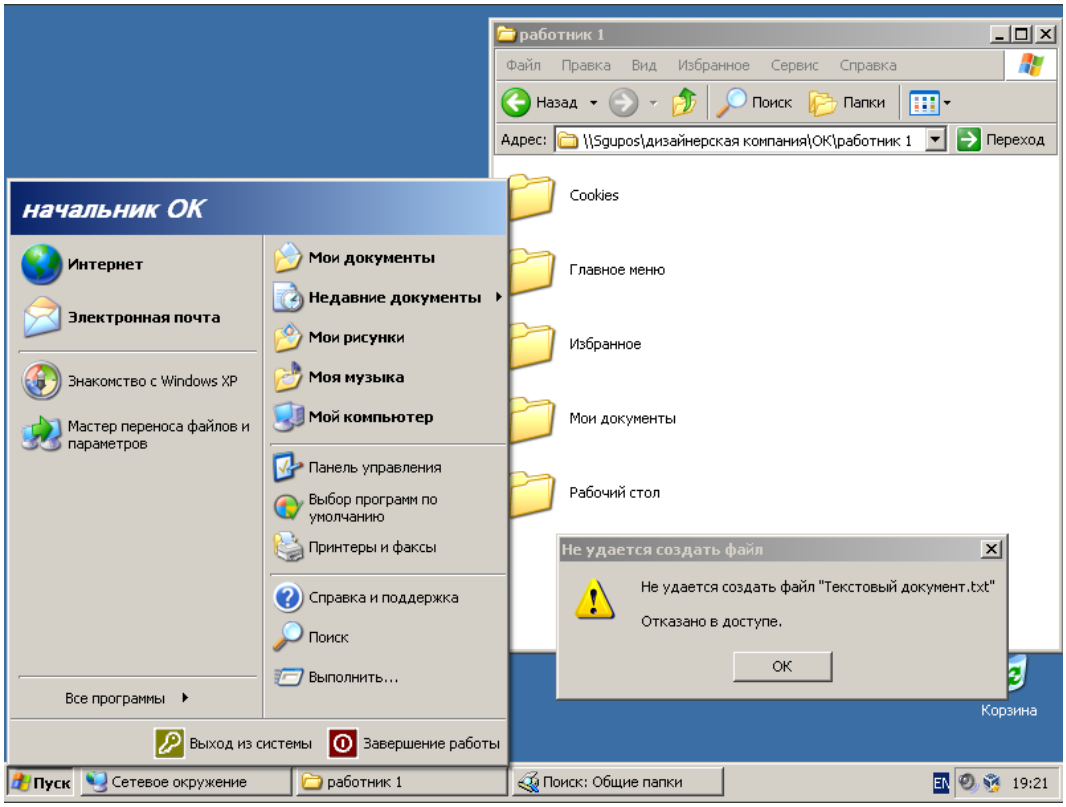

Рисунок 31 – Попытка создания объекта без права на это.

Попытка удаления файлов в папке «Работник ОК 2» пользователем «Начальник ОК» вызовет следующее окно (Рисунок 32). Соответствующий аудит отказа представлен на рисунке 33.

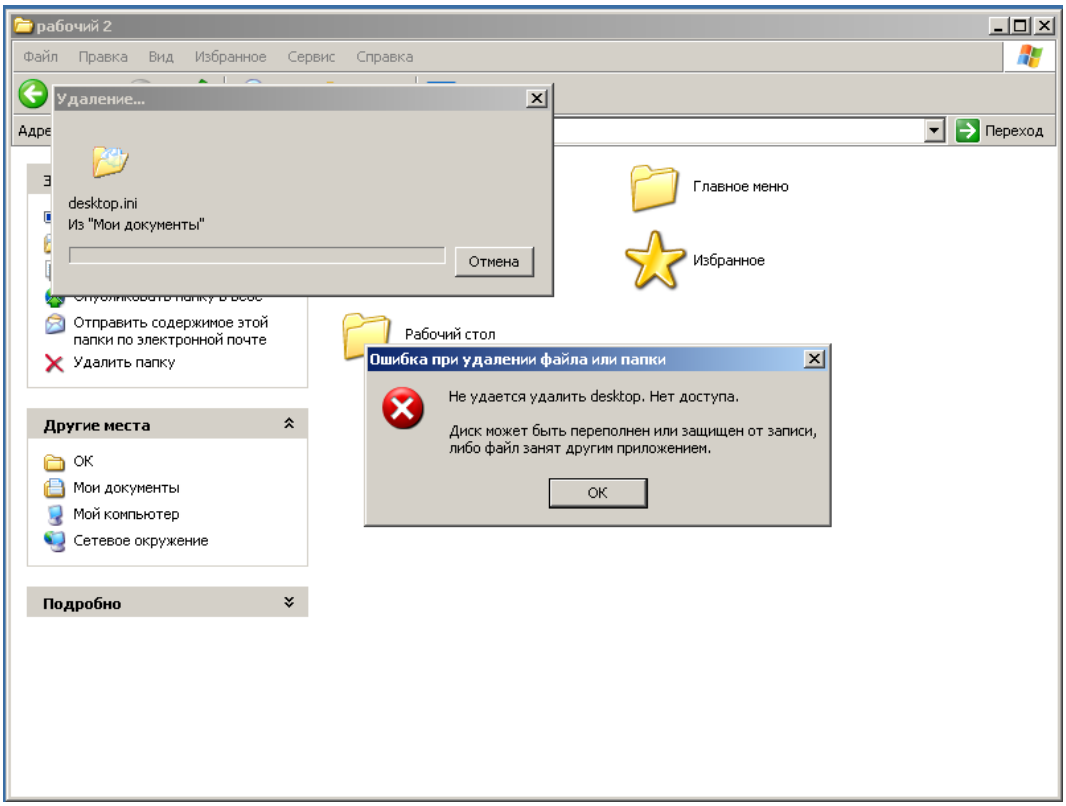

Рисунок 32 – Попытка удаления объекта без права на это.

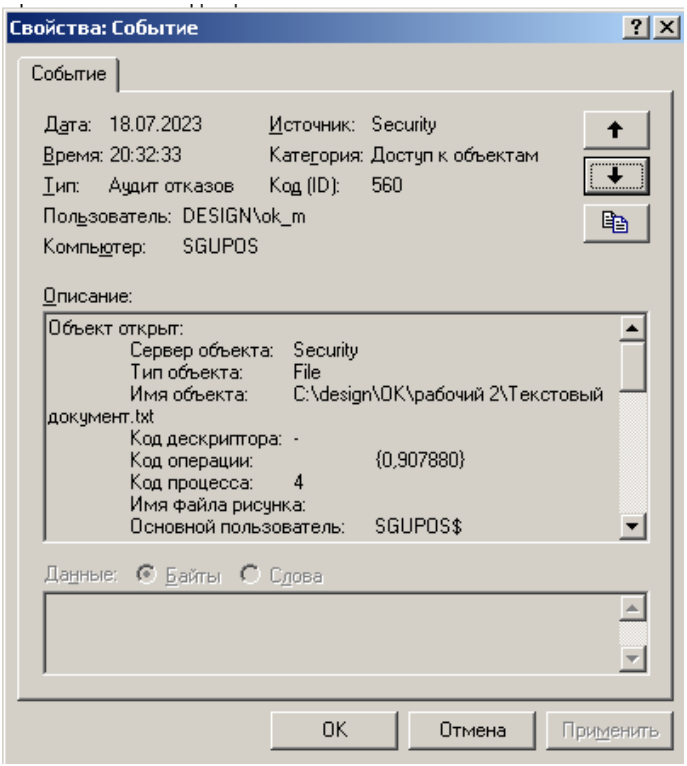

Рисунок 33 – Аудит отказа удаления файла.

4. Действия по изменению ПРД

Для настройки аудита по изменению ПРД необходимо включить «Аудит изменения политики» (Рисунок 34). Так же необходимо настроить аудит в свойствах папки, который был применен в предыдущем пункте (пункт 3 настройки РД СВТ).

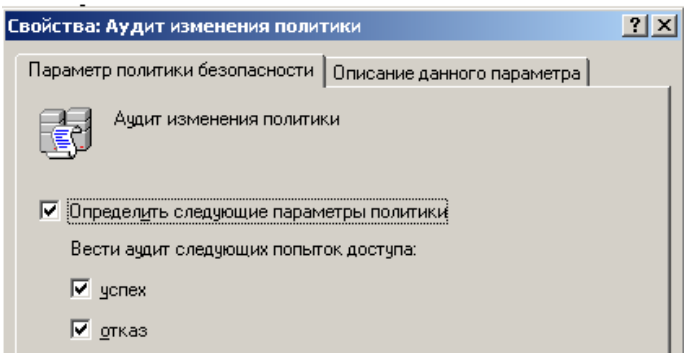

Рисунок 34 – Настройка аудита изменения ПРД.

Попробуем изменить права доступа для файла в общей папке для пользователя «ОК рабочий 2» от пользователя «Начальник ОК», как показано на рисунке 35.

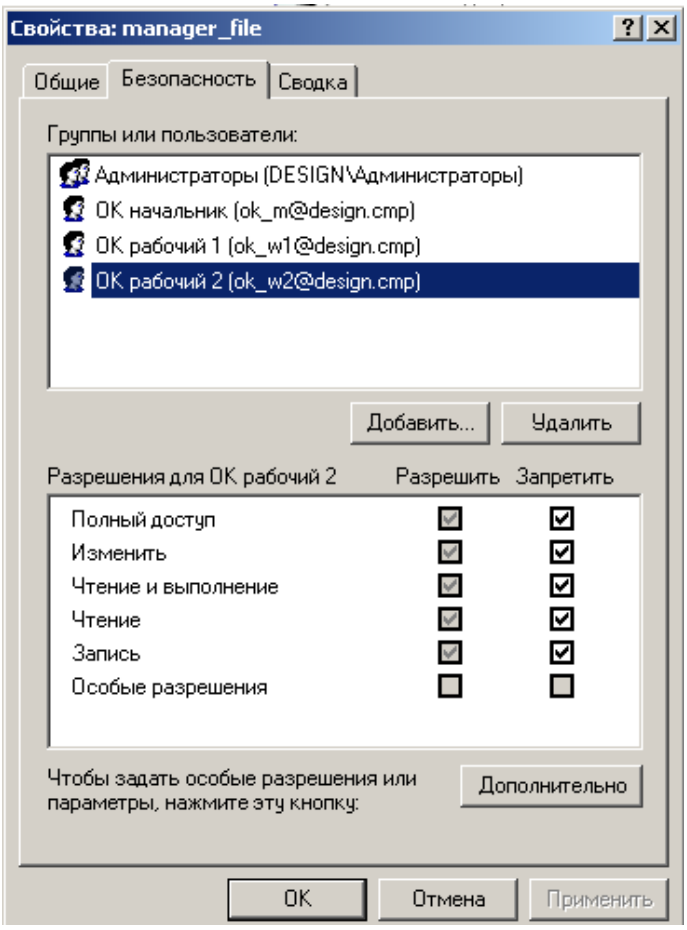

Рисунок 35 – Изменение прав доступа.

На рисунке 36 представлен аудит изменения объекта, для которого меняли ПДР, а именно путь, пользователь, который менял ПРД и какой доступ предоставил

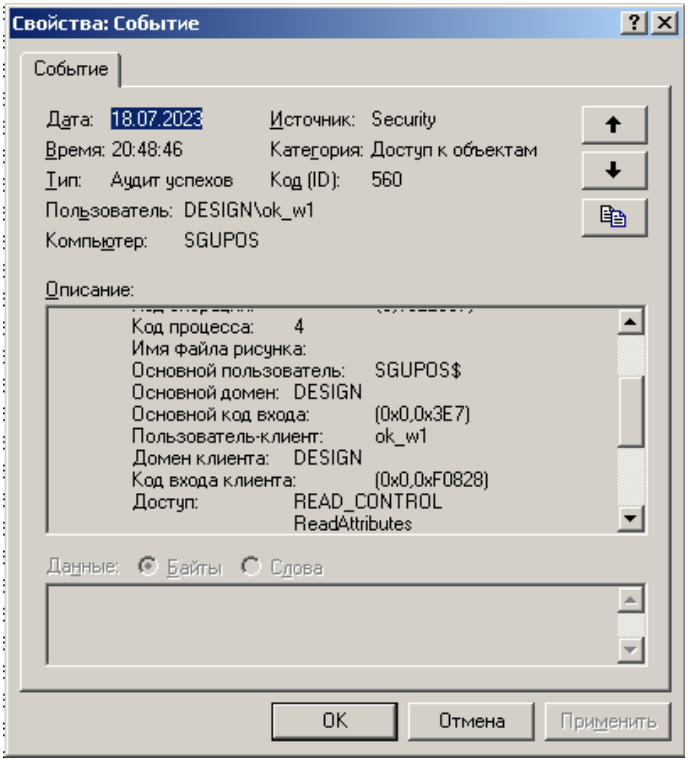

Рисунок 36 – Аудит изменения прав доступа.

Реализуем требования согласно Приказу № 21 ФСТЭК.

1. Следующие требования обеспечиваются организационными мерами:

• определение событий безопасности, подлежащих регистрации, и сроков их хранения;

• определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

• сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

2. Защита информации о событиях безопасности

С помощью групповых политик запретим доступ к журналам системы локальной группе гостей (Рисунок 37).

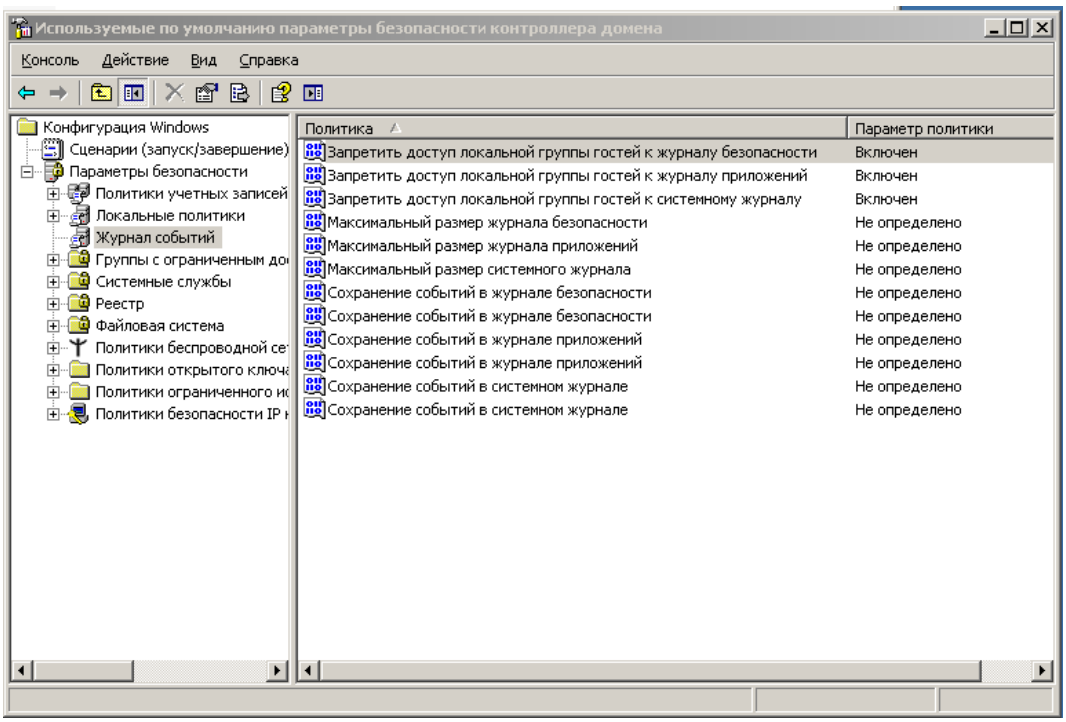

Рисунок 37 – Запрет доступа к журналам событий.

Установим права доступа к журналу (Рисунок 38).

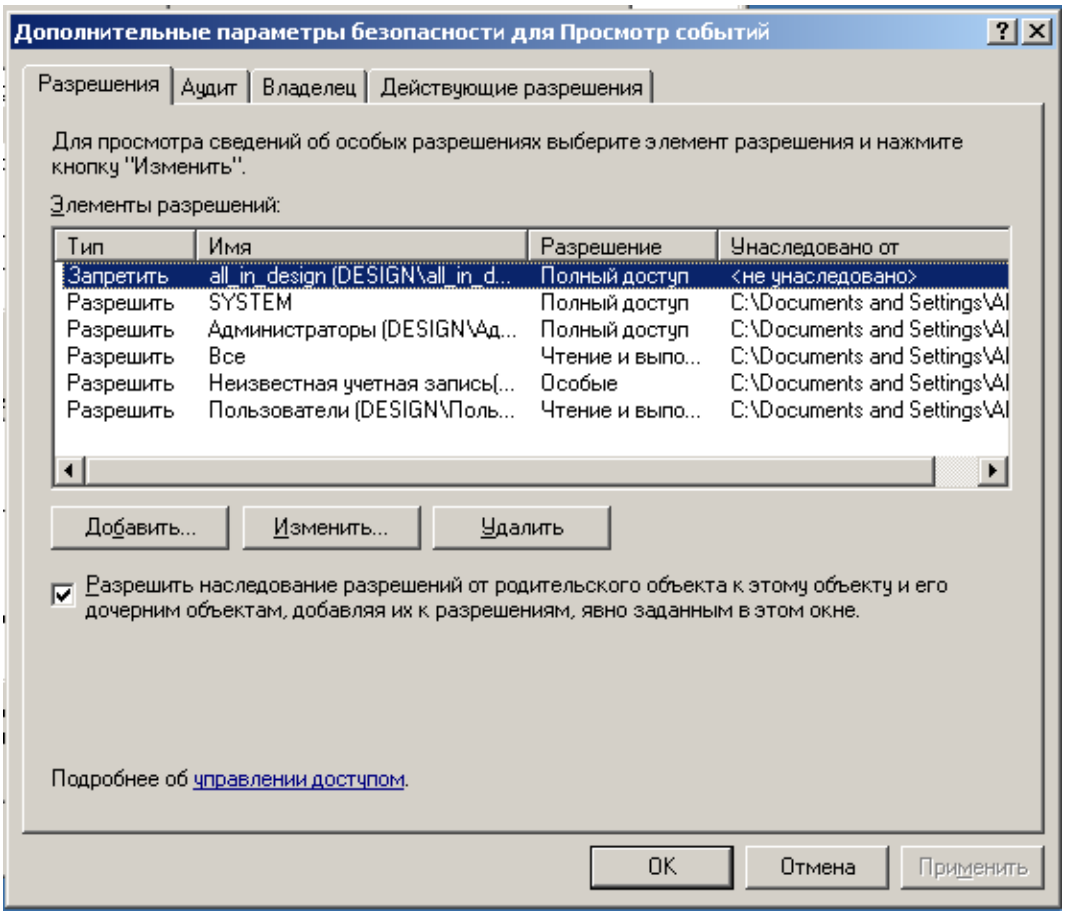

Рисунок 38 – Разграничение прав доступа к журналу событий.

И установим аудит отказов для журнала (Рисунок 39).

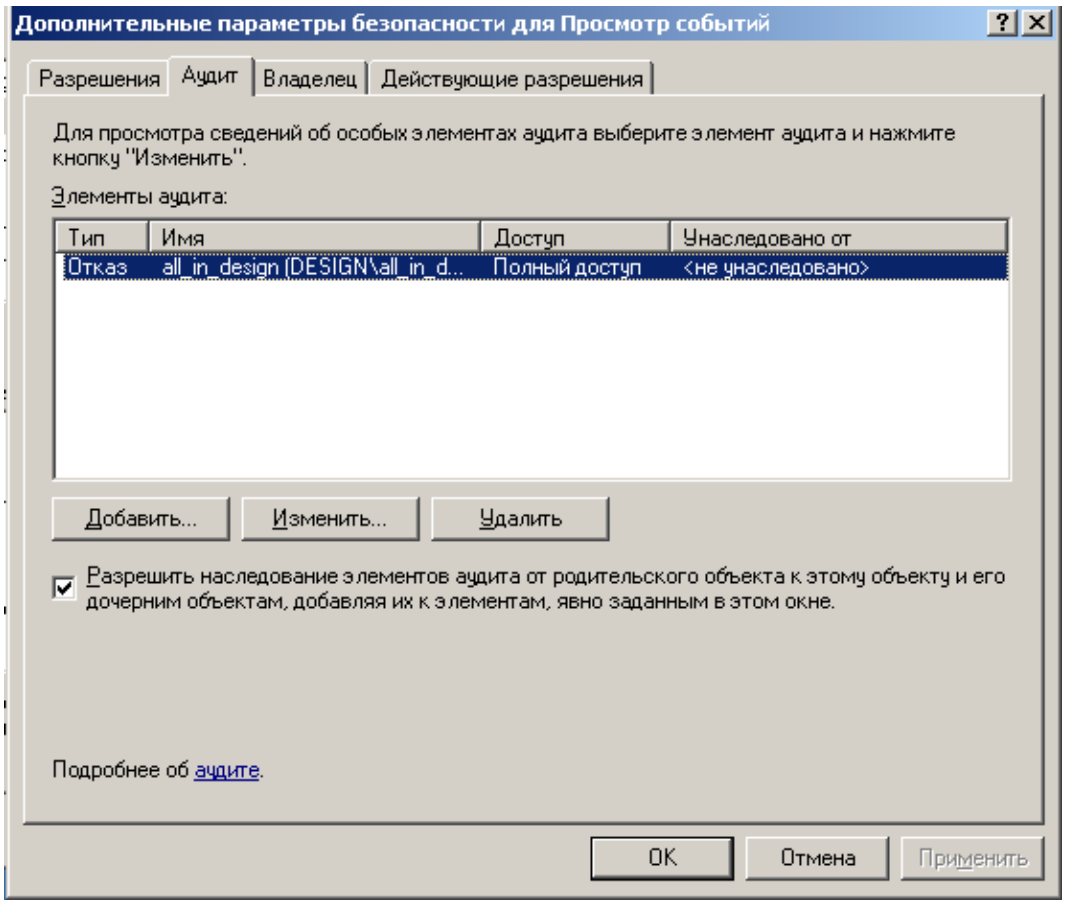

Рисунок 39 – Аудит журнала событий.

Требования к системе из ПП № 1119 также обеспечиваются организационными мерами.

Заключение

В ходе работы была рассмотрена работа межсетевого экрана, классификация типов межсетевых экранов по способу размещения и их недостатки.

При выполнении практической части работы были изучены основные руководящие документы, приказы и Постановления Правительства, включающие в себя требования к автоматизированным системам, средствам вычислительной техники и информационным системам персональных данных. Также в практической части была настроена подсистема регистрации и учёта в домене на базе Windows Server 2003 с учетом требований безопасности, предъявляемых к информационной системе, согласно требуемому уровню защищенности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Межсетевые экраны и VPN [Электронный ресурс] // Эшелон– компьютерная безопасность [Электронный ресурс]. URL: https://npo echelon.ru/production/66/ (дата обращения: 03.07.2023). Загл. с экрана. Яз. рус.
2. Безопасность сетей. Лекция 10, стр.1,2 [Электронный ресурс] // Национальный Открытый Институт [Электронный ресурс]. URL: http://www.intuit.ru/studies/courses/102/102/lecture/2989 (дата обращения: 03.07.2023). Загл. с экрана. Яз. рус.
3. Межсетевые экраны. [Электронный ресурс] // Руководство FreeBSD [Электронный ресурс] URL: https://www.freebsd.org/doc/ru/books/handbook/firewalls.html (дата обращения: 03.07.2023). Загл. с экрана. Яз. рус.
4. Принципы работы межсетевых экранов. [Электронный ресурс] // Руководство FreeBSD [Электронный ресурс] URL: https://www.freebsd.org/doc/ru/books/handbook/firewalls-concepts.html (дата обращения: 03.07.2023). Загл. с экрана. Яз. рус.
5. Способы организации защиты [Электронный ресурс] // Компьютер-пресс [Электронный ресурс]. URL: http://compress.ru/article.aspx?id=10145 (дата обращения: 03.07.2023). Загл. с экрана. Яз. рус.
6. Максимов, В. Межсетевые экраны. Способы организации защиты [Электронный ресурс] // Компьютер-пресс [Электронный ресурс]. URL: http://compress.ru/article.aspx?id=10145 (дата обращения: 03.07.2023). Загл. с экрана. Яз. рус.
7. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс] / ФСТЭК России [Электронный ресурс]. URL: 45 https://fstec.ru/component/attachments/download/296 (дата обращения: 06.07.2023). Загл. с экрана. Яз. Рус.

8. Специальные требования и рекомендации по технической защите конфиденциальной информации [Электронный ресурс] / Эксперт [Электронный ресурс]. URL: http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm (дата обращения: 06.07.2023). Загл. с экрана. Яз. Рус.
9. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс] / ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru/component/attachments/download/297 (дата обращения: 06.07.2023). Загл. с экрана. Яз. Рус.
10. Приказ от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] / ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 06.07.2023). Загл. с экрана. Яз. Рус.
11. Постановление от 1 ноября 2012 г. №1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] / КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=137356&fld=134&dst=1000000001,0&rnd=0.5588456717278638#05600955382203672 (дата обращения: 06.07.2023). Загл. с экрана. Яз. Рус