ЗАО «АЛТЭКС-СОФТ»

Операционная система Microsoft® Windows Server™ 2003 Standard Edition Service Pack 2

Руководство по безопасной настройке и контролю сертифицированной версии

2010

СОДЕРЖАНИЕ

1 Введение

Настоящий документ содержит рекомендации по настройке и контролю механизмов защиты операционных систем (ОС) семейства Microsoft® Windows Server™ 2003 при организации обработки конфиденциальной информации на объекте информатизации. Представленные рекомендации применимы для сертифицированных по требованиям безопасности операционных систем:

- Microsoft® Windows Server™ 2003 Standard Edition Service Pack 2;
- Microsoft® Windows Server™ 2003 Standard Edition R2 Service Pack 2;

(далее по тексту руководства – ОС Microsoft® Windows Server 2003).

Руководство предназначено для настройки механизмов защиты ОС Microsoft® Windows Servertм 2003 в соответствии с той конфигурацией, в которой данное изделие было сертифицировано, а также подготовки объекта информатизации к аттестации на соответствие требованиям безопасности при обработке конфиденциальной информации.

Операционная система Microsoft® Windows Servertм 2003 может функционировать как на автономном компьютере (ПЭВМ), так и на компьютере в составе локальной вычислительной сети, логическая инфраструктура которой базируется на основе службы каталогов Microsoft® Active Directory™. В этом случае компьютер с установленной на нем ОС Microsoft® Windows Servertм 2003 может быть включен в состав участников домена Active Directory (и таким образом, управление политиками безопасности для него будет осуществляться централизованно), либо не входить в него, но иметь возможность сетевого взаимодействия с другими компьютерами в составе домена. Взаимодействие компьютера в данной конфигурации с остальными будет эквивалентно взаимодействию компьютеров в составе рабочей группы (Workgroup). В этом случае компьютер будет функционировать так же как автономный, и управление его параметрами безопасности будет осуществляться посредством локальной политики безопасности.

При включении компьютера с установленной на нем операционной системой Microsoft® Windows Servertм 2003 в состав домена Active Directory он может выступать в качестве контроллера домена либо в качестве рядового сервера (member server), реализующего одну из ролей:

- сервера служб сетевой инфраструктуры:
  - сервера протокола динамической настройки узлов (Dynamic Host Configuration Protocol);
  - сервера служб имен Интернета для Windows (Windows Internet Name Service);
  - сервера служб доменных имен (Domain Name Service);

– файлового сервера;
– сервера печати;
– сервера служб Интернета (Internet Information Services);
– сервера служб проверки подлинности в Интернете (Internet Authentication Services);
– сервера служб сертификации (Certificate Services).

К рассматриваемому множеству ролей, которые могут быть реализованы компьютером под управлением операционной системой Microsoft® Windows Servertм 2003 , дополнительно следует отнести роль бастион-хоста (bastion host), в качестве которого обычно выступают компьютеры, расположенные в выделенном пограничном сегменте вычислительной сети (демилитаризованной зоне) и доступные извне (из сетей общего доступа), что подразумевает использование ими более ограничивающей политики безопасности и применение усиленных настроек безопасности.

Каждый из рассматриваемых вариантов функционирования операционной системы Microsoft® Windows Servertм 2003 предусматривает две сертифицированные конфигурации безопасности:

– «Enterprise Client» (EC);
– «Specialized Security – Limited Functionality» (SSLF).

В случае функционирования операционной системы Microsoft® Windows Servertм 2003 на автономном компьютере (компьютере в составе рабочей группы), выступающем в качестве бастион-хоста, ее параметры безопасности определяются только конфигурацией «Specialized Security – Limited Functionality».

Конфигурация «Enterprise Client»

Данная конфигурация подразумевает наличие инфраструктуры домена Active Directory, в состав которого включены компьютеры, функционирующие только под управлением операционных систем семейства Microsoft® Windows® 2000, Microsoft® Windows® 2003 Server, Microsoft® Windows® Vista, Microsoft® Windows Server™ 2008 и Microsoft® Windows® XP Professional. Управление серверами и клиентскими компьютерами в данной среде происходит через использование групповой политики, предоставляющей механизм централизованного управления политиками безопасности для среды функционирования в целом. Применение групповой политики при этом осуществляется на различных уровнях иерархии каталога Active Directory (домены, организационные подразделения), что позволяет определять как общие для всех пользователей и компьютеров

домена, так и специфичные для конкретной конфигурации и исполняемой роли, параметры безопасности.

Конфигурация «Specialized Security – Limited Functionality»

Конфигурация «Specialized Security – Limited Functionality» подразумевает наличие более ограничивающей политики безопасности и усиленные настройки безопасности для серверов под управлением операционной системы Microsoft® Windows Servertм 2003 по сравнению с конфигурацией «Enterprise Client». При применении данных настроек безопасности функциональность пользователя ограничивается полномочиями на выполнение только необходимых задач.

В каждом конкретном случае выбор конфигурации безопасности определяется исходя из критерия «безопасность-производительность».

Таким образом, исходя из рассмотренных режимов функционирования и конфигураций безопасности, можно выделить следующие варианты функционирования операционной системы Microsoft® Windows Servertм 2003 (см. таблицу 1.1).

Таблица 1.1 – Варианты функционирования операционной системы Microsoft® Windows Servertм 2003

№ п/п	Варианты функционирования операционной системы
ОС Microsoft® Windows Servertм 2003 на компьютере в составе домена Active Directory в конфигурации «Enterprise Client»	
1.	Компьютер в конфигурации «Enterprise Client», функционирующий в качестве контроллера домена.
2.	Компьютер в конфигурации «Enterprise Client», функционирующий в качестве рядового сервера домена.
ОС Microsoft® Windows Servertм 2003 на компьютере в составе домена Active Directory в конфигурации «Specialized Security – Limited Functionality»	
3.	Компьютер в конфигурации «Specialized Security – Limited Functionality», функционирующий в качестве контроллера домена.
4.	Компьютер в конфигурации «Specialized Security – Limited Functionality», функционирующий в качестве рядового сервера домена.
ОС Microsoft® Windows Server™ 2003 на компьютере, являющимся автономным	
5.	Автономный компьютер в конфигурации «Specialized Security – Limited Functionality», функционирующий в качестве бастион-хоста.

ⓘ ВНИМАНИЕ:

Представленные в настоящем руководстве рекомендации по настройке механизмов защиты ОС Microsoft® Windows Servertм 2003 должны быть предварительно протестированы и апробированы в тестовой среде перед их применением в действующей вычислительной среде организации, в рамках которой предполагается функционирование ПЭВМ под управлением указанной ОС, настроенной в соответствии с сертифицированной конфигурацией безопасности.

2 Последовательность действий по настройке сертифицированной версии операционной системы Microsoft® Windows Server™ 2003

2.1 Общие указания по настройке параметров безопасности сертифицированной версии операционной системы Microsoft® Windows Servertм 2003

Для настройки параметров безопасности сертифицированной версии операционной системы Microsoft® Windows Servertм 2003 администратор эксплуатирующей организации (администратор безопасности) может воспользоваться инструментальным средством «Мастер настройки безопасности» (Security Configuration Wizard) и механизмами, реализуемыми групповой политикой. Совместное использование указанных средств позволяет обеспечить большую управляемость, гибкость, комплексность подхода и согласованность в процессе управления настройками параметров безопасности компьютеров под управлением ОС Microsoft® Windows Servertм 2003 .

2.1.1 Мастер настройки безопасности

«Мастер настройки безопасности» представляет собой инструментальное средство, позволяющее обеспечить снижение количества возможных атак в отношении компьютеров, функционирующих под управлением операционных систем семейства Microsoft® Windows Servertм 2003 . Основным назначением «Мастера настройки безопасности» является предоставление администратору безопасности возможности быстрого и точного определения требуемой функциональности, реализуемой данным компьютером, и последующее конфигурирование системы в соответствии с выполняемой компьютером ролью. С использованием «Мастера настройки безопасности» администратор безопасности может создавать, тестировать, отлаживать и развертывать политики безопасности, которые отключают ненужную функциональность ОС Microsoft® Windows Servertм 2003 , обеспечивая тем самым большую защищенность компьютера.

«Мастер настройки безопасности» позволяет выполнять настройку:

- параметров системных служб (исходя из реализуемых компьютером ролей);
- параметров сетевой безопасности системы (брандмауэра Windows и IPSec);
- параметров реестра;
- политики аудита;
- служб IIS.

Создаваемая с использованием «Мастера настройки безопасности» политика безопасности базируется на определенных для данного компьютера ролях (например,

файлового сервера или сервера печати). При этом созданная политика может быть протестирована и применена как к указанному компьютеру, так и к другим компьютерам, реализующим роли, аналогичные ролям выбранного сервера.

Роль компьютера определяется набором системных служб, открытыми сетевыми портами и требованиями к службам IIS, необходимыми для выполнения указанной роли. Список системных служб, порты для входящего сетевого трафика и другие параметры, требуемые для реализации каждой роли, отличаются. В результате политики безопасности, создаваемые «Мастером настройки безопасности» для серверов, выполняющих различные роли, также различаются.

Политики, создаваемые «Мастером настройки безопасности», представляют собой файлы в формате XML (для хранения которых используется папка `%systemdir%\security\msscw\Policies`), в которых могут содержаться параметры для системных служб, брандмауэра Windows, IPSec, значений реестра, политики аудита, служб IIS, а также параметры безопасности, импортируемые из предопределенных шаблонов безопасности.

Развертывание созданной политики безопасности может осуществляться с помощью:

- графического интерфейса «Мастера настройки безопасности», делающим процедуру настройки наиболее простой и интуитивно понятной;
- утилиты командной строки `Scwcmd.exe`.

При этом с использованием графического интерфейса «Мастера настройки безопасности» администратор безопасности может осуществить как создание политики безопасности требуемой конфигурации, так и ее применение. Однако с помощью «Мастера настройки безопасности» политика безопасности в один момент времени может быть применена только к одному компьютеру.

В случае необходимости применения единой политики безопасности к определенному множеству компьютеров, реализующих одинаковую функциональность (например, ко всем файловым серверам организации), без использования механизма групповой политики, обеспечиваемого службой каталогов Active Directory, необходимо использовать утилиту командной строки `Scwcmd.exe`. Основным недостатком данного метода распространения политики безопасности является необходимость вручную указывать имя требуемой политики и имена компьютеров, к которым ее требуется применять, что повышает вероятность ошибки при выполнении данной операции. Кроме того, если имеется ряд компьютеров с отличающейся конфигурацией (например, набором автоматически запускаемых системных служб или открытых сетевых портов), администратор безопасности вынужден будет создавать отдельные политики для каждого компьютера и также по отдельности их применить. Исходя из указанных выше ограничений по применению

утилиты командной строки `Scwcmd.exe` ее использование для развертывания политик безопасности рекомендуется ограничить.

2.1.2 Групповая политика

Операционная система Microsoft® Windows Servertм 2003 сертифицирована в конфигурациях безопасности «Enterprise Client» и «Specialized Security – Limited Functionality» для вариантов функционирования, перечисленных в таблице 1.1.

Для реализации политик безопасности, соответствующих конфигурациям «Enterprise Client» или «Specialized Security – Limited Functionality», администратор эксплуатирующей организации может настроить параметры безопасности (см. Приложение А) самостоятельно, либо (что является более предпочтительным) использовать предопределенные значения параметров безопасности, представленные в файлах шаблонов безопасности, размещенных на компакт-диске, входящем в комплект поставки сертифицированной версии операционной системы Microsoft® Windows Servertм 2003 или в Центе сертификационных обновлений производителя сертфицированной версии ПО http://www.altx-soft.ru/downloads.htm. Использование шаблонов безопасности позволяет упростить выполнение задач администрирования, поскольку обеспечивает приведение к единой конфигурации безопасности заданного множества компьютеров в рамках одного домена.

По умолчанию, на компьютерах под управлением операционной системы Microsoft® Windows Servertм 2003 для хранения шаблонов безопасности используется папка `%SystemRoot%\security\templates`. Данная папка не реплицируется между контроллерами домена. Таким образом, во избежание возникновения проблем с управлением версиями шаблонов безопасности, должно быть определено место для организации централизованного хранения оригинала шаблонов (как правило, для этой цели используется какой-либо из контроллеров домена или выделенный файловый сервер). Оптимальной является практика, когда изменения всегда вносятся в одну и ту же копию шаблонов безопасности. Оригинальную копию шаблонов безопасности необходимо хранить в защищенном от несанкционированного доступа месте, доступ к которому предоставляется только администраторам.

Настройку параметров безопасности компьютера под управлением операционной системы Microsoft® Windows Servertм 2003 , являющегося членом домена Active Directory, в соответствии с конфигурациями «Enterprise Client» или «Specialized Security – Limited Functionality» (см. Приложение А) необходимо осуществлять через использование групповых политик, применяемых на уровне домена и организационных подразделений (контейнеров, содержащих учетные записи компьютеров), что позволит всем компьютерам,

на которые распространяется групповая политика, автоматически применить единую конфигурацию безопасности.

Альтернативой централизованному применению групповой политики является настройка каждого компьютера вручную. Рекомендованные для конфигураций «Enterprise Client» и«Specialized Security – Limited Functionality» (см. Приложение А) позволят обеспечить безопасность компьютеров под управлением операционной системы Microsoft® Windows Servertм 2003 , и создать среду, защищенную от большинства современных угроз безопасности, обеспечив тем самым эффективное и непрерывное предоставление ими требуемых сервисов и услуг.

Таким образом, в зависимости от режимов функционирования (в автономном режиме или в составе домена Active Directory) шаблоны безопасности необходимо включать либо в локальный объект групповой политики, либо в объекты групповой политики.

ⓘ **Примечание**:

В данном случае предполагается, что объекты групповой политики, базируемые на Active Directory, будут создаваться с использованием утилиты командной строки `Scwcmd.exe` на основе политик безопасности, формируемых «Мастером настройки безопасности».

Соответствие возможных вариантов функционирования операционной системы Microsoft® Windows Servertм 2003 и применяемых шаблонов безопасности приведено в таблице 2.1.

Таблица 2.1 – Соответствие возможных вариантов функционирования ОС Microsoft® Windows Servertм 2003 и применяемых шаблонов безопасности

№ п/п	Роли, реализуемые компьютером	Конфигурация безопасности «Enterprise Client»	Конфигурация безопасности «Specialized Security – Limited Functionality»
1.	Контроллер домена	WS03-EC-Domain.inf	WS03-SSLF-Domain.inf
		WS03-EC-Domain-Controller.inf	WS03- SSLF-Domain-Controller.inf
2.	Рядовой сервер домена	WS03-EC-Domain.inf	WS03-SSLF-Domain.inf
		WS03-EC-Member-Server.inf	WS03-SSLF-Member-Server.inf
3.	Бастион-хост	Вариант функционирования не предусмотрен	WS03-SSLF-Bastion-Host.inf

2.2 Порядок применения объектов групповой политики для компьютеров, являющихся членами домена Active Directory

Порядок применения объектов групповой политики строго иерархичен и по умолчанию предусматривает наследование от структурных объектов Active Directory высокого уровня к объектам более низкого уровня. Групповые политики применяются в следующем порядке:

1. **Local group policy** – локальная групповая политика;
2. **Site-level group policies** – групповые политики, применяемая на уровне сайта (область вычислительной сети, обеспечивающей объединение контроллеров домена высокоскоростными и надежными каналами связи);
3. **Domain-level group policies** - групповые политики, применяемая на уровне домена Active Directory;
4. **OU-level group policies** – групповые политики уровня организационного подразделения (ОП - это контейнер, используемый для объединения объектов домена в логические административные группы).

Применению групповой политики, содержащей параметры безопасности, соответствующие сертифицированным конфигурациям «Enterprise Client» или «Specialized Security – Limited Functionality», должно предшествовать выполнение ряда подготовительных операций, а именно:

- создание иерархии организационных подразделений, содержащих учетные записи компьютеров с установленной операционной системой Microsoft® Windows Servertм 2003 , выполняющих одинаковые роли;
- создание на уровне домена объекта групповой политики и импортирование в него шаблона безопасности, определяющего политику учетных записей и используемого для конфигурирования общих для всех компьютеров домена параметров безопасности;
- преобразование политик безопасности, созданных с использованием «Мастера настройки безопасности», в соответствующие объекты групповой политики (ОГП);
- осуществление привязки созданных ОГП к конкретным организационным подразделениям.

Иерархия организационных подразделений предусматривает создание администратором необходимого количества контейнеров, содержащих учетные записи компьютеров, реализующих единые роли. В частности, в рамках одного организационного подразделения должны быть объединены учетные записи компьютеров с установленной операционной системой Microsoft® Windows Servertм 2003 , реализующих одну из предопределенных в данном руководстве ролей, например, роль сервера служб сетевой инфраструктуры. В свою очередь данные организационные подразделения, учитывающие специфику реализуемой компьютером роли, должны быть объединены в рамках единого родительского ОП, что позволит применить к указанным компьютерам параметры безопасности, общие для всех рядовых серверов в рамках домена.

Иерархия создаваемых объектов групповой политики должна базироваться на существующей иерархии ОП и предусматривать следующие уровни:

- **Domain Level** – объект групповой политики данного уровня устанавливает политику учетных записей и используется для конфигурирования общих для всего домена параметров безопасности;
- **Baseline Level** – объекты групповой политики, применяемые на данном уровне, задают параметры безопасности, общие для рядовых серверов в рамках всего домена. Привязка объекта групповой политики данного уровня осуществляется к организационному подразделению, объединяющему учетные записи всех рядовых серверов, реализующих предопределенные роли;
- **Role Specific Level** – на данном уровне определяются параметры безопасности, учитывающие особенности, связанные с выполнением компьютером определенной роли. Поскольку требования безопасности, предъявляемые к одним серверам (например, к серверам служб сетевой инфраструктуры), могут отличаться от требований, предъявляемым к другим серверам (например, к серверам служб Интернета IIS), групповая политика должна быть определена для каждой роли серверов, что влечет за собой необходимость создания отдельного ОГП для каждого ОП, содержащего учетные записи компьютеров, реализующих одну из предопределенных ролей.

Структурная схема иерархии организационных подразделений и сопоставленных с ними объектов групповой политики с учетом импортируемых шаблонов безопасности на примере конфигурации «Enterprise Client» представлена на рисунке 2.1.

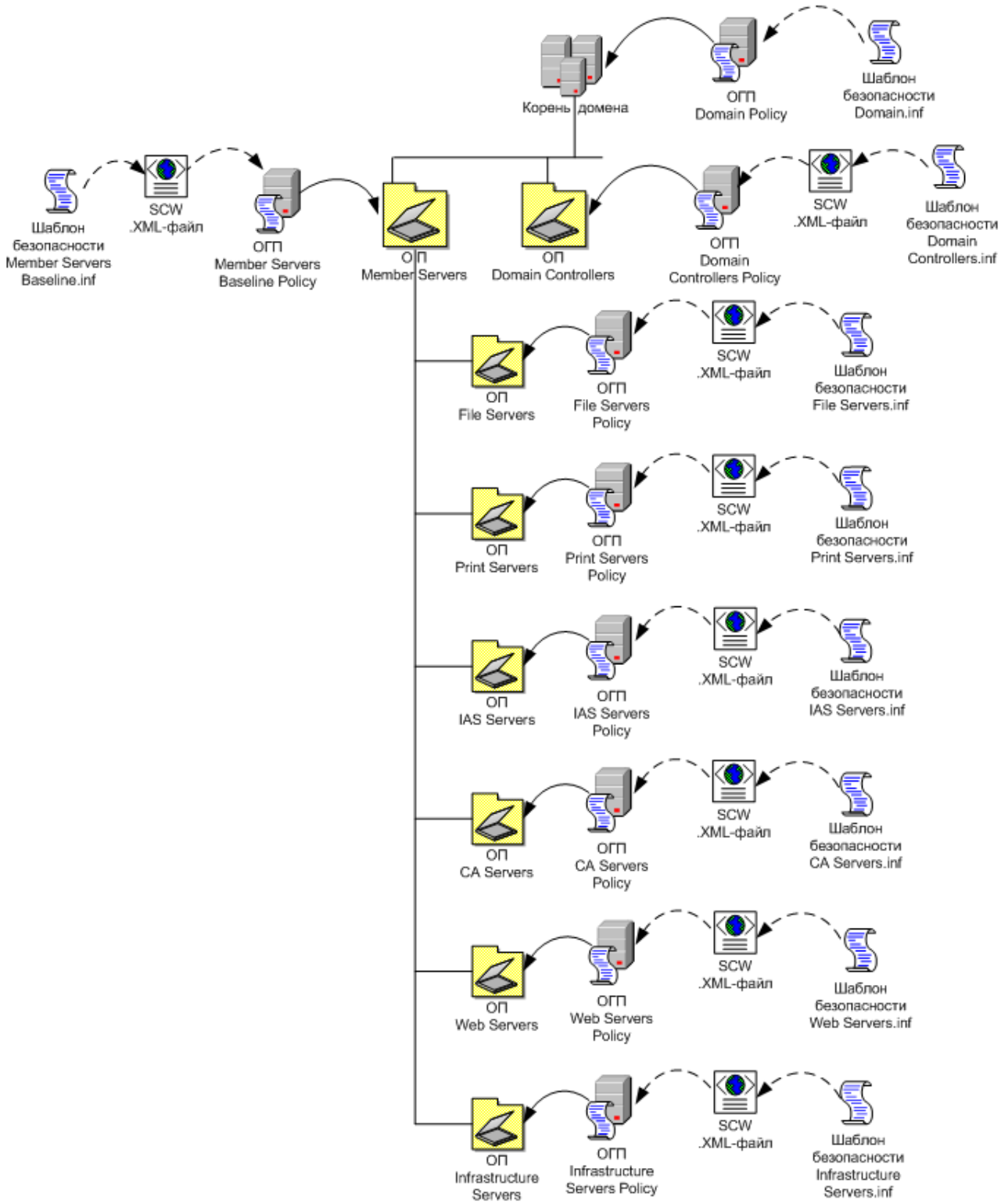


Рисунок 2.1 – Иерархия ОП и применяемых ОГП

2.3 Общее описание порядка настройки компьютера в предопределенной конфигурации безопасности

Предпочтительным способом настройки компьютера в соответствии с сертифицированной конфигурацией безопасности, исходя из выполняемой им роли, является совместное использование рассмотренных выше средств, предусматривающее:

- создание и тестирование политики безопасности с использованием графического интерфейса «Мастера настройки безопасности»;
- преобразование с использованием утилиты командной строки `Scwcmd.exe` полученной политики безопасности в объект групповой политики (файлы политик в формате XML, созданные «Мастером настройки безопасности», преобразуются в форматы, распознаваемые различными расширениями групповой политики);
- осуществление привязки созданных объектов групповой политики к конкретным организационным подразделениям в иерархии структурных объектов Active Directory, что позволит обеспечить применение единых параметров безопасности к компьютерам под управлением операционной системы Microsoft® Windows Servertм 2003 в соответствии с требуемыми конфигурациями безопасности.

ⓘ **Примечание**:

Применение политик, созданных «Мастером настройки безопасности», на компьютерах, функционирующих под управлением ОС более ранних версий, чем Microsoft® Windows Server™ 2003 Service Pack 2/ Microsoft® Windows Server™ 2003 R2 Service Pack 2, не поддерживается. Следует использовать возможности фильтров WMI групповой политики, чтобы политики, созданные «Мастером настройки безопасности», не применялись на компьютерах, функционирующих под управлением ОС более ранних версий.

Таким образом, для настройки компьютеров в предопределенной конфигурации безопасности в данном руководстве предлагается применить комбинированный подход, в рамках которого объединены преимущества использования «Мастера настройки безопасности» и механизма групповой политики. Это позволит администраторам эксплуатирующих организаций обеспечить простоту создания, тестирования и отладки конфигураций безопасности, а также гибкость и масштабируемость, которые требуются при управлении большими вычислительными сетями на базе Microsoft® Windows.

В общем случае процесс настройки компьютеров под управлением ОС Microsoft® Windows Servertм 2003 в предопределенной конфигурации безопасности с учетом реализуемой ими роли предусматривает выполнение следующих действий:

1. Создание иерархии организационных подразделений, содержащих учетные записи компьютеров с установленной операционной системой Microsoft® Windows Servertм 2003 , выполняющих одинаковые роли (см. рисунок 2.1).
2. Настройку групповой политики, определяемой на уровне домена Active Directory.
3. Создание и тестирование с использованием «Мастера настройки безопасности» базовой политики безопасности (baseline policy), определяющей общие для всех рядовых серверов в рамках домена параметры и настройки безопасности.
4. Преобразование полученной политики безопасности в ОГП и его привязка к соответствующему организационному подразделению, объединяющему учетные записи всех рядовых серверов, реализующих предопределенные роли.
5. Создание и тестирование с использованием «Мастера настройки безопасности» политик безопасности, учитывающих особенности, связанные с выполнением компьютером предопределенной серверной роли.
6. Преобразование полученных политик безопасности в ОГП и их привязка к соответствующим организационным подразделениям, содержащим учетные записи компьютеров, реализующих одну из предопределенных ролей.

2.3.1 Общий порядок создания политики безопасности с использованием «Мастера настройки безопасности»

Создание политики безопасности с использованием инструментального средства «Мастер настройки безопасности» должно осуществляться на компьютере с вновь инсталлированной операционной системой Microsoft® Windows Servertм 2003 . Это позволит обеспечить отсутствие нелегитимного программного обеспечения и непротиворечивость выполняемых настроек безопасности. Данный компьютер должен входить в состав домена Active Directory и иметь набор всего необходимого для выполнения им своей роли программного обеспечения.

Для создания политики безопасности администратор эксплуатирующей организации должен выполнить следующие действия:

1. Установить «Мастер настройки безопасности». Для этого нажать кнопку «Пуск», выбрать «Панель управление» и далее «Установка и удаления программ». В диалоговом окне

«Установка и удаления программ» выбрать пункт меню «Установка компонент Windows». В появившемся окне «Мастера компонентов Windows» выбрать компонент «Мастер настройки безопасности» и нажать «Далее». В последующем следовать появляющимся на экране указаниям по установке инструментального средства «Мастер настройки безопасности».

2. По окончанию установки запустить «Мастер настройки безопасности» и в качестве выполняемого действия выбрать «Создать новую политику безопасности» (см. рисунок 2.2). Нажать «Далее».

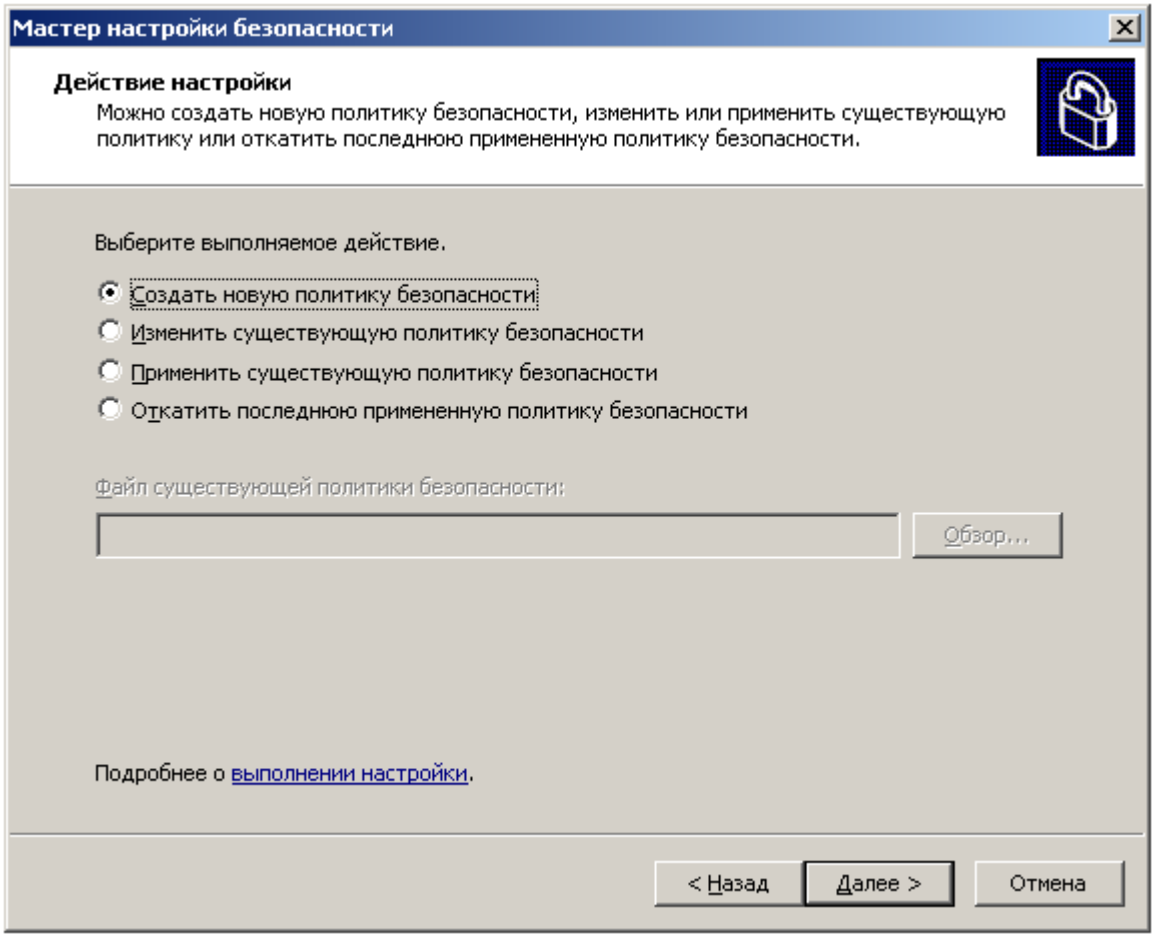


Рисунок 2.2

3. Выбрать сервер (ввести DNS-имя, NetBIOS-имя или IP-адрес компьютера), который будет использоваться в качестве образца (reference computer) для создаваемой политики безопасности, и нажать «Далее».

4. По окончанию обработки базы данных настройки безопасности нажать «Далее».

5. В разделе выбора ролей осуществить выбор требуемых ролей сервера, выполняемых данным компьютером (см. рисунок 2.3), и нажать «Далее».

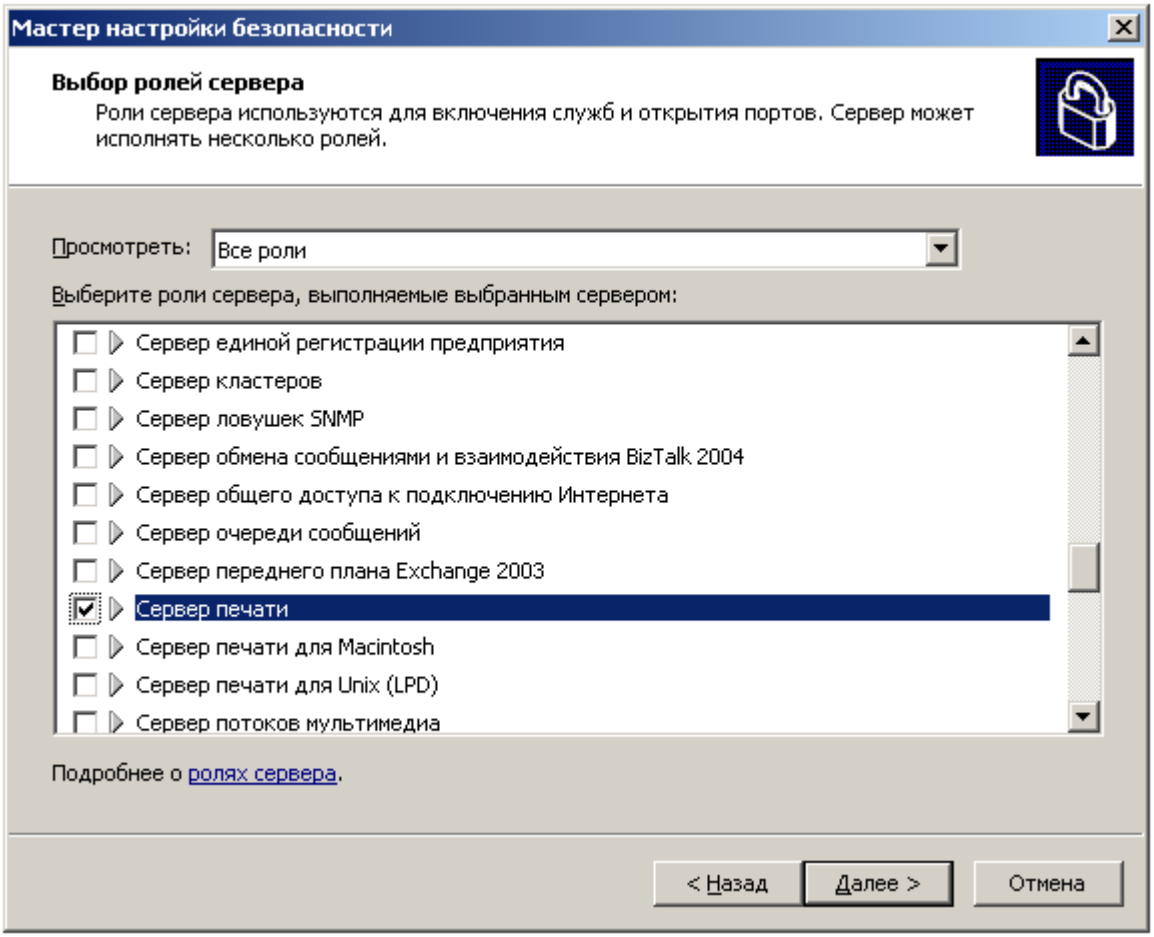


Рисунок 2.3

6. В разделе выбора клиентских возможностей необходимо убедиться в правильности выбранных клиентских возможностей, которые могут реализовываться данным сервером (см. рисунок 2.4), и нажать «Далее». Клиентские возможности сервера определяются требуемым для соответствующих ролей набором системных служб.

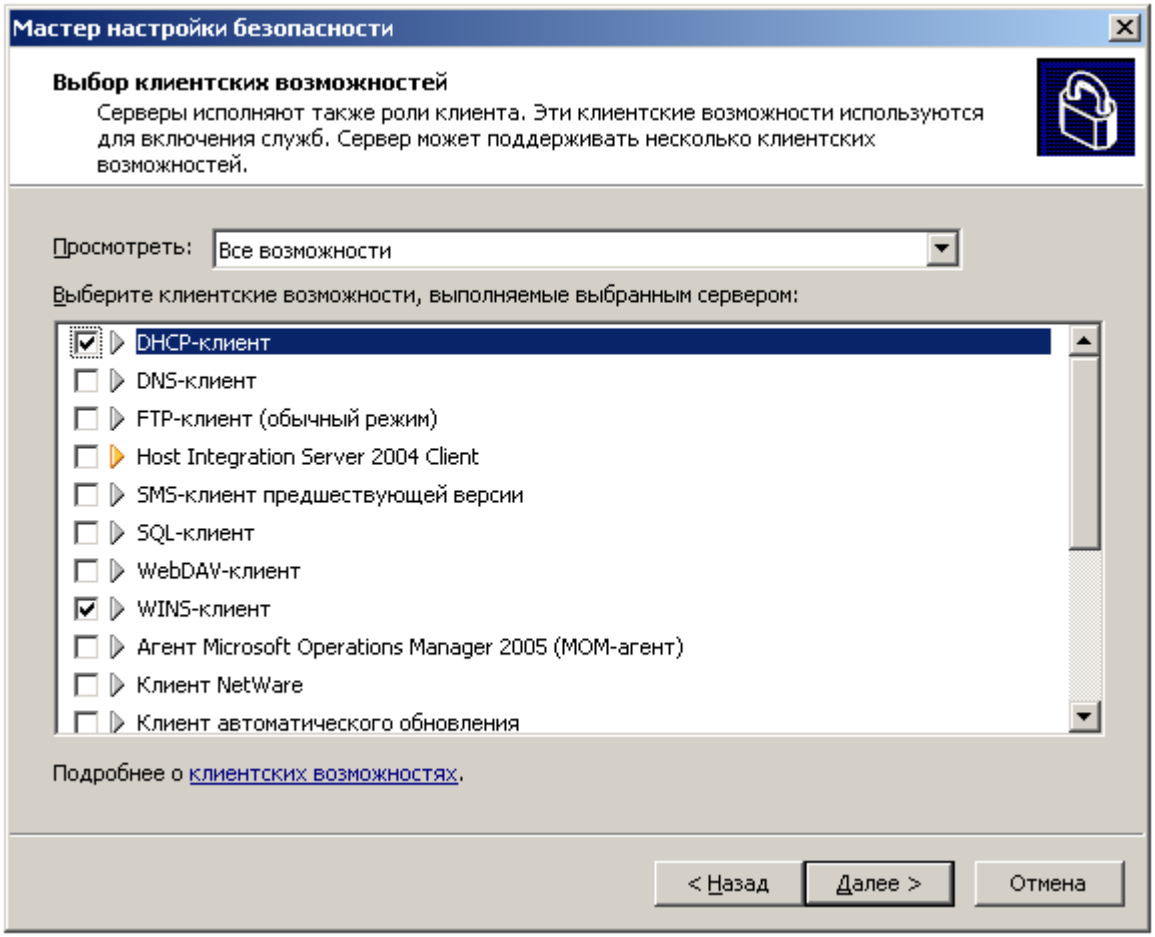


Рисунок 2.4

7. С учетом требований вычислительной среды осуществить выбор необходимых возможностей администрирования, используемых администратором безопасности для управления выбранным сервером, и нажать «Далее».

8. Выбрать дополнительные службы, которые требуются для данного сервера, и нажать «Далее».

9. На странице «Обработка неопределенных служб» произвести настройку режима запуска служб, которые отсутствуют в базе данных настройки безопасности «Мастера настройки безопасности» и не установлены в настоящее время на сервере, используемом в качестве образца для создания политики безопасности, но которые могут быть установлены на других компьютерах, на которых планируется применять создаваемую политику безопасности.

10. На странице «Подтверждение изменений для служб» просмотреть список вех изменений, вносимых данной политикой безопасности в работу системных служб на выбранном сервере, и в случае согласия нажать «Далее» (см. рисунок 2.5).

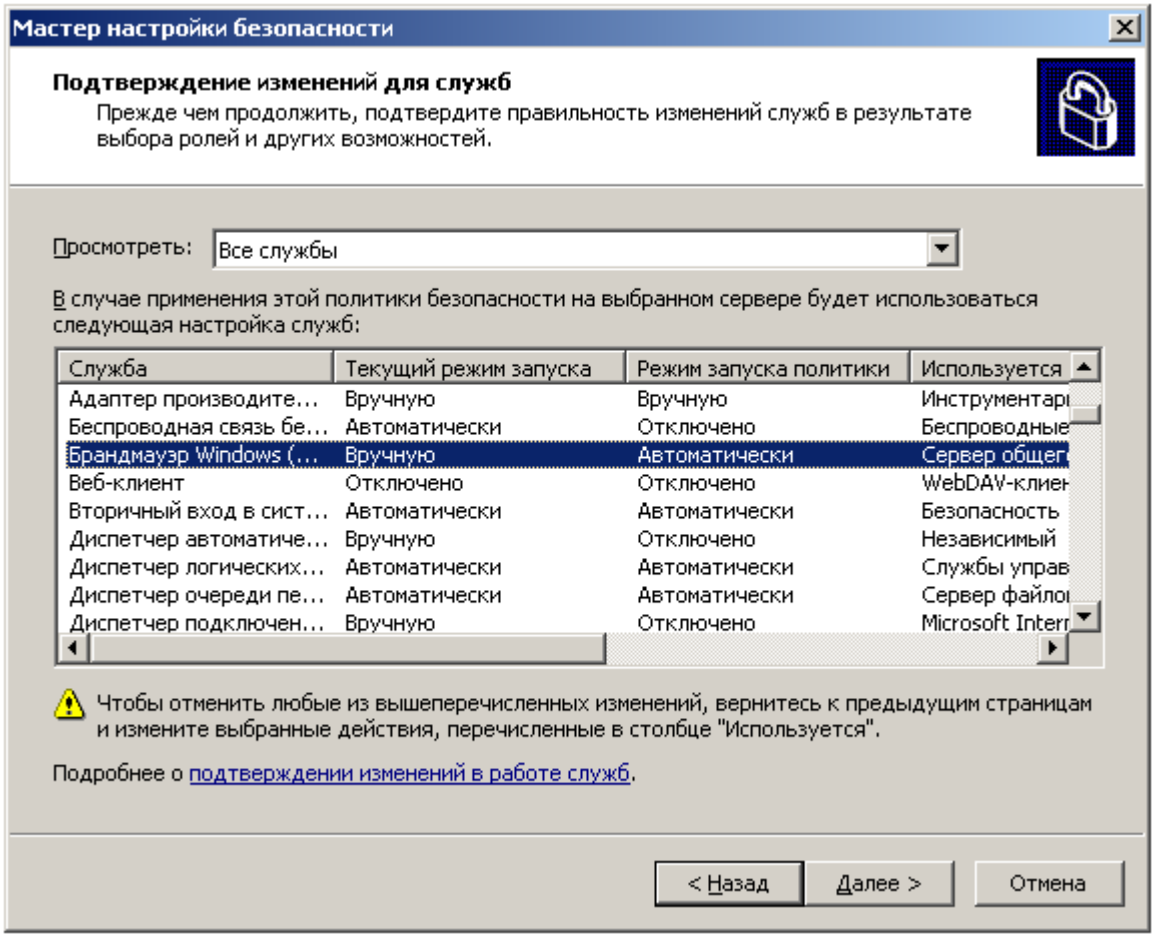


Рисунок 2.5

11. В разделе настройки сетевой безопасности на странице «Открытие портов и одобрение приложений» осуществить требуемую настройку брандмауэра Windows, перечислив необходимые сетевые порты, которые должны быть открыты, исходя из реализуемых компьютером ролей, запущенных приложений и решаемых административных задач (см. рисунок 2.6). Нажать «Далее».

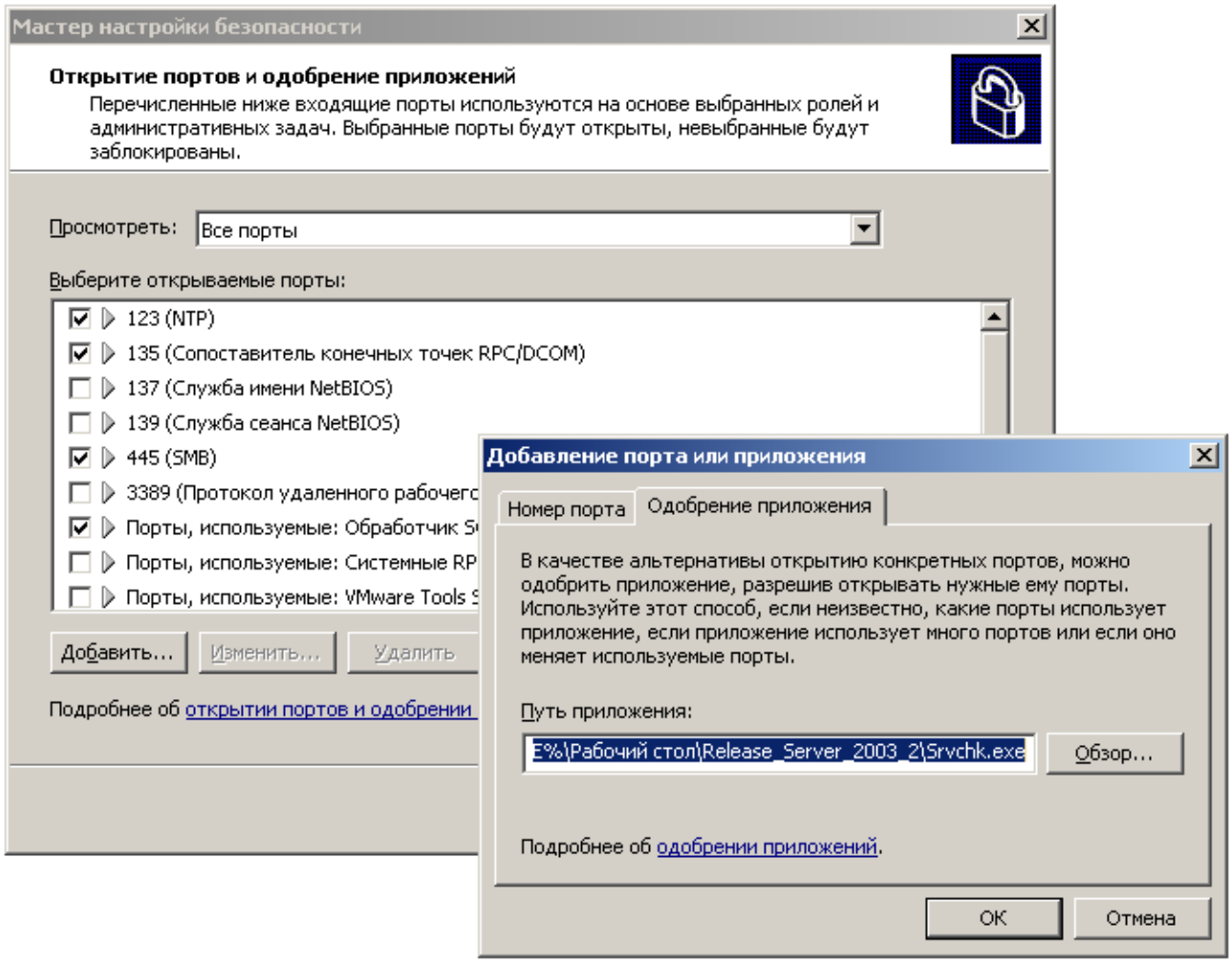


Рисунок 2.6

12. Выполнить подтверждение параметров настройки сетевых портов и нажать «Далее».

13. Пропустить настройку разделов «Параметры реестра» и «Политика аудита», с использованием «Мастера настройки безопасности», выбрав опцию «Пропустить этот раздел» (см. рисунок 2.7).

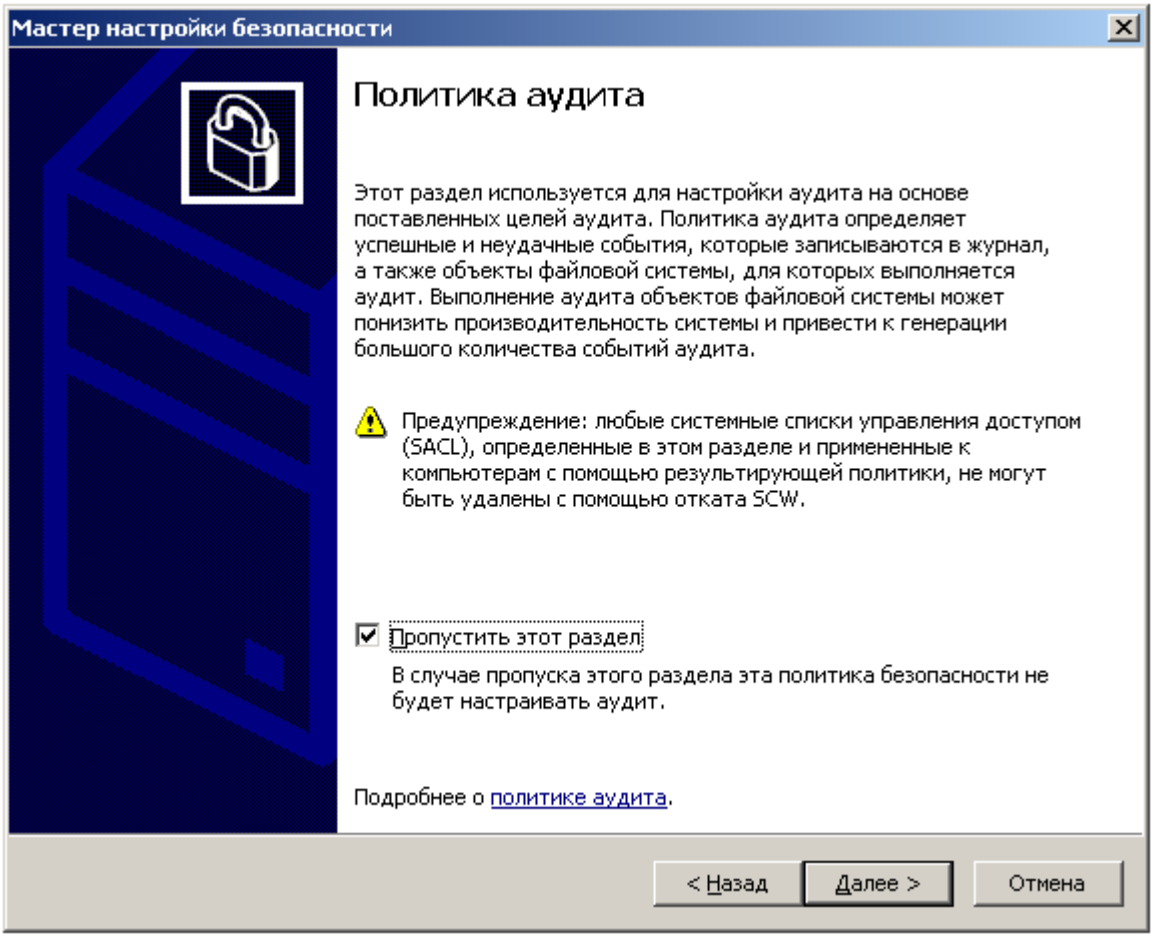


Рисунок 2.7

14. На странице задания имени файла политики безопасности включить в политику соответствующий шаблон безопасности, исходя из реализуемой компьютером роли (см. таблицу 2.1). Для этого нажать «Включение шаблонов безопасности…» и посредством кнопки «Добавить» выбрать соответствующий шаблон безопасности, который необходимо включить в созданную политику безопасности для последующей настройки серверов в требуемой конфигурации безопасности (см. рисунок 2.8).

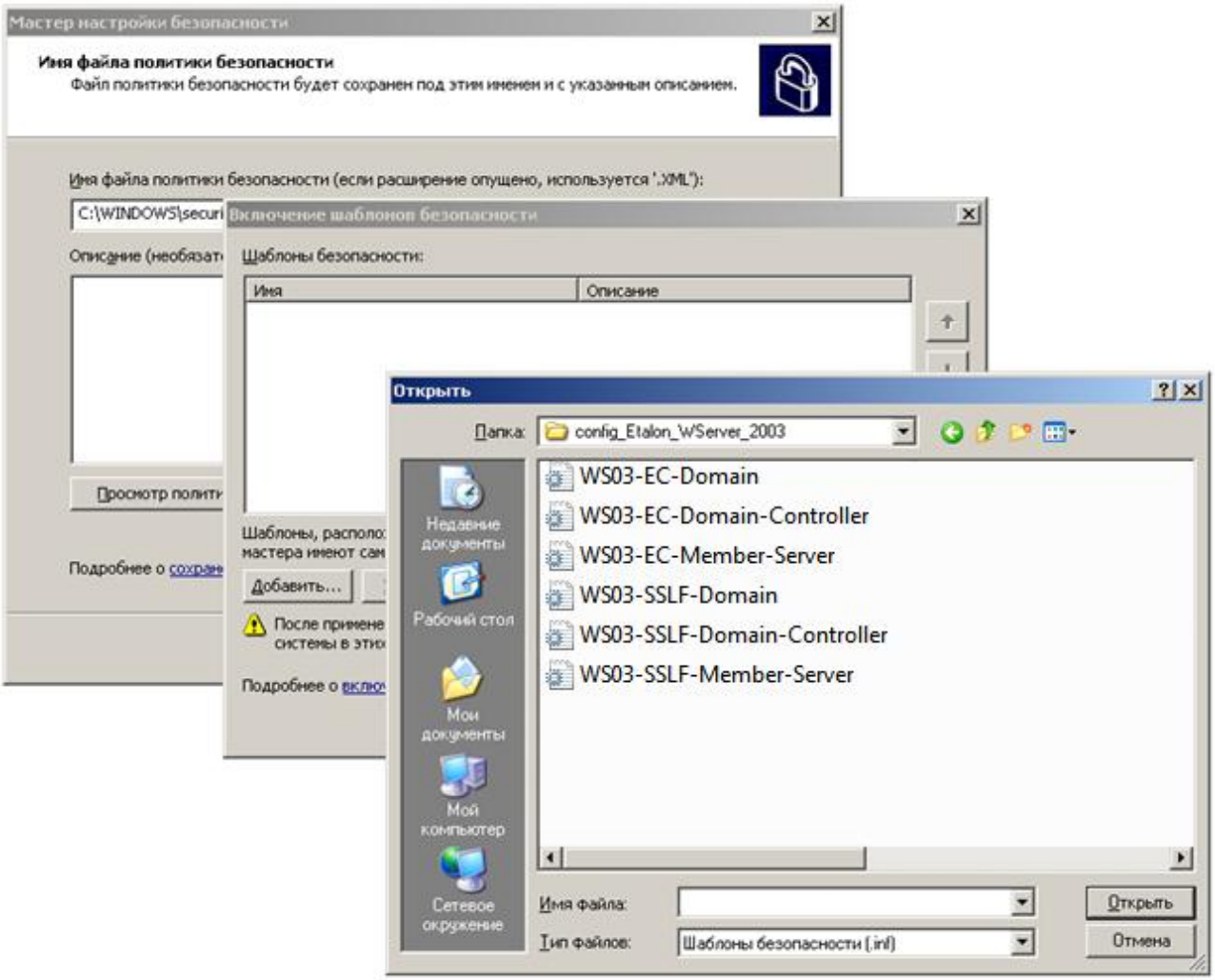


Рисунок 2.8

15. На странице выбора вариантов применения созданной политики безопасности выбрать опцию «Применять позже», нажать «Далее» и завершить работу «Мастера настройки безопасности».

Примечание:

По окончанию создания политики безопасности администратору безопасности рекомендуется провести тестирование созданной политики в тестовой среде с целью оценки степени ее влияния на функциональность серверов, на которых предполагается ее применение. Использование данного подхода поможет выявить и зафиксировать потенциальные проблемы, которые могут возникнуть при применении политики безопасности (например, в случае запрета запуска служб, которые необходимы для функционирования сервера).

2.3.2 Порядок преобразование политики безопасности в ОГП

Для преобразования политики безопасности, созданной с использованием «Мастера настройки безопасности», в объект групповой политики в командной строке необходимо осуществить запуск утилиты `Scwcmd.exe` со следующими параметрами:

```
scwcmd transform /p:<Путь_к_Файлу_политики.xml> /g:<Имя_ОГП>
```

ⓘ **Примечание**:

- Для выполнения операций преобразования необходимо обладать административными полномочиями в системе (учетная запись, с использованием которой осуществлялся вход в систему, должна быть членом группы безопасности «Администраторы домена»).
- Операция преобразования должна выполняться с сервера, входящего в домен, в котором будет применен объект групповой политики.

Пример преобразования политики безопасности `FileServer.xml`, созданной с использованием «Мастера настройки безопасности», в объект групповой политики с именем `FileServersGPO` с использованием утилиты командной строки `Scwcmd.exe` представлен на рисунке 2.9.

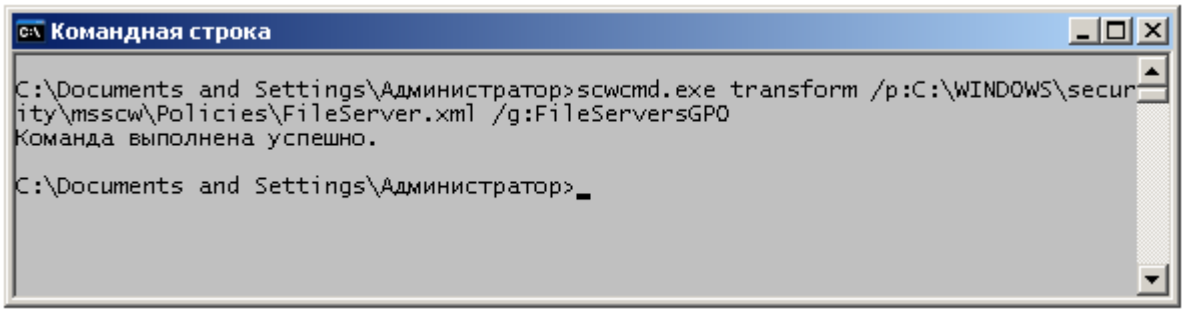


Рисунок 2.9.

По окончанию создания объекта групповой политики администратор безопасности должен осуществить привязку полученного ОГП к соответствующему организационному подразделению, содержащему учетные записи серверов, реализующих одну из предопределенных ролей. Это позволит применить к серверам, реализующих одинаковую роль, единую политику безопасности.

2.4 Настройка компьютера, являющегося членом домена Active Directory, в конфигурации «Enterprise Client»

2.4.1 Используемые шаблоны безопасности

Для автоматической настройки параметров политики учетных записей следует импортировать шаблон безопасности WS03-EC-Domain.inf в требуемый объект групповой политики, определяемый на уровне домена (в частности, в ОГП «Default Domain Policy» - политика домена, используемая по умолчанию), на контроллере домена под управлением операционной системы Microsoft® Windows Server 2003™.

Для настройки общих для всех рядовых серверов в рамках домена параметров безопасности необходимо с использованием «Мастера настройки безопасности» создать соответствующую политику (см. пп.2.3.1 настоящего Руководства), учитывающей требуемые аспекты безопасности, и включить в нее шаблон безопасности WS03-EC-Member-Server.inf Далее с использованием утилиты командной строки `Scwcmd.exe` преобразовать полученную политику в соответствующий объект групповой политики и осуществить его привязку к организационному подразделению, содержащему учетные записи всех рядовых серверов домена (ОП «Member Servers»), реализующих предопределенные роли (см. рисунок 2.1).

Для настройки параметров безопасности, учитывающих особенности, связанные с выполнением компьютером определенной роли, необходимо с использованием «Мастера настройки безопасности» дополнительно создать соответствующую политику безопасности, включив в нее требуемый шаблон безопасности (см. таблицу 2.2). Далее с использованием утилиты командной строки `Scwcmd.exe` преобразовать полученную политику в ОГП и осуществить его привязку к организационному подразделению, содержащему учетные записи компьютеров, реализующих одинаковую роль. Соответствие между реализуемыми компьютером под управлением ОС Microsoft® Windows Servertм 2003 в конфигурации «Enterprise Client» ролями и включаемыми в политики безопасности шаблонами представлено в таблице 2.2.

Таблица 2.2 - Соответствие возможных вариантов функционирования ОС Microsoft® Windows Servertм 2003 в конфигурации «Legacy Client» и применяемых шаблонов безопасности

№ п/п	Роли, реализуемые ОО	Применяемые шаблоны безопасности
1.	Контроллер домена	WS03-EC-Domain-Controller.inf
2.	Сервер служб сетевой инфраструктуры	WS03-EC-Member-Server.inf
3.	Файловый сервер	
4.	Сервер печати	
5.	Сервер служб Интернета	
6.	Сервер служб проверки подлинности	
7.	Сервер служб сертификации	

2.4.2 Порядок применения шаблонов безопасности и объектов групповой политики

Импорт шаблона безопасности WS03-EC-Domain.inf необходимо осуществлять с использованием редактора соответствующего объекта групповой политики, определяемого на уровне домена (например, ОГП «Default Domain Policy»). Чтобы импортировать шаблон безопасности в соответствующий ОГП необходимо выполнить следующие действия:

1. Нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду `dsa.msc` и нажать «ОК».

2. В появившемся окне оснастки консоли управления «Active Directory – пользователи и компьютеры» выделить имя домена (например, `domain-name.com`) и посредством пункта «Свойства» контекстного меню получить доступ к диалоговому окну свойств существующего домена. Далее, перейти на вкладку «Групповая политика» (см. рисунок 2.10).

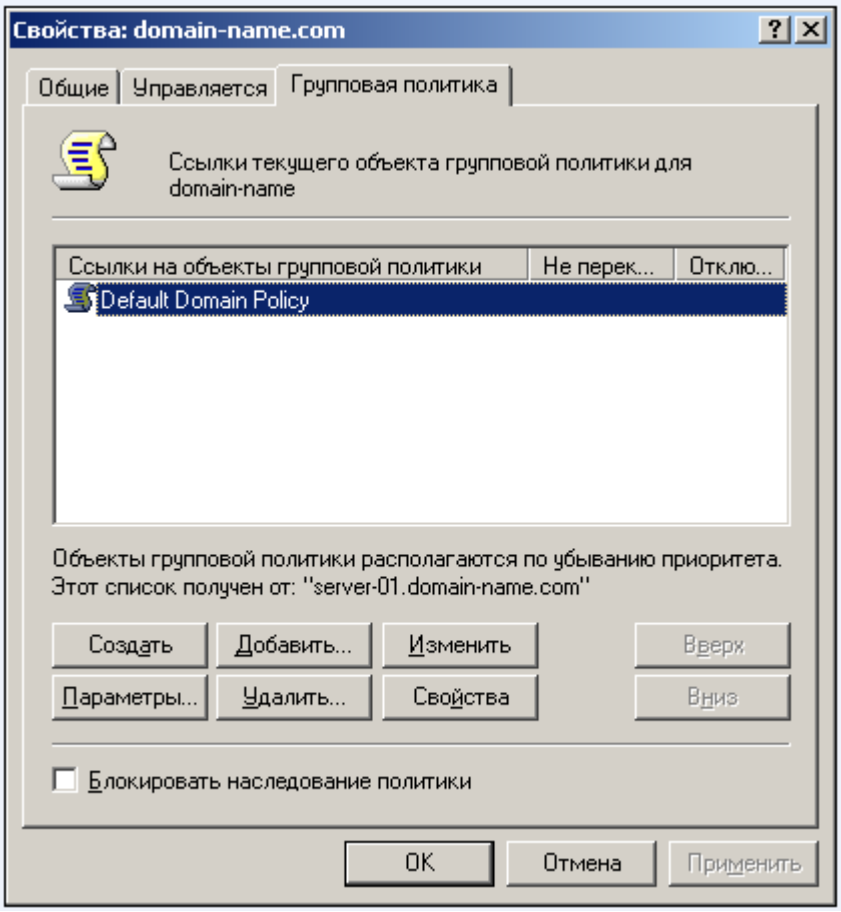


Рисунок 2.10

3. Вызвать редактор объектов групповой политики (Group Policy Object Editor). Для этого необходимо выбрать требуемый объект групповой политики, определяемый на уровне домена, (в частности, ОГП «Default Domain Policy») и нажать «Изменить». В случае если существует необходимость, администратором на уровне домена может быть создан новый объект групповой политики с привязкой к указанному домену. Для этого в окне свойств существующего домена на вкладке «Групповая политика» следует нажать «Создать» и ввести имя нового объекта групповой политики.

4. В окне редактора объектов групповой политики выбрать узел «Конфигурация компьютера» и перейти к разделу «Конфигурация Windows».

5. Выделить папку «Параметры безопасности» и посредством контекстного меню выбрать пункт «Импорт политики».

6. В появившемся диалоговом окне импорта политики выбрать шаблон безопасности WS03-EC-Domain.inf, и нажать кнопку «Открыть». После чего параметры безопасности импортируются из выбранного файла в текущий объект групповой политики (см. рисунок 2.11).

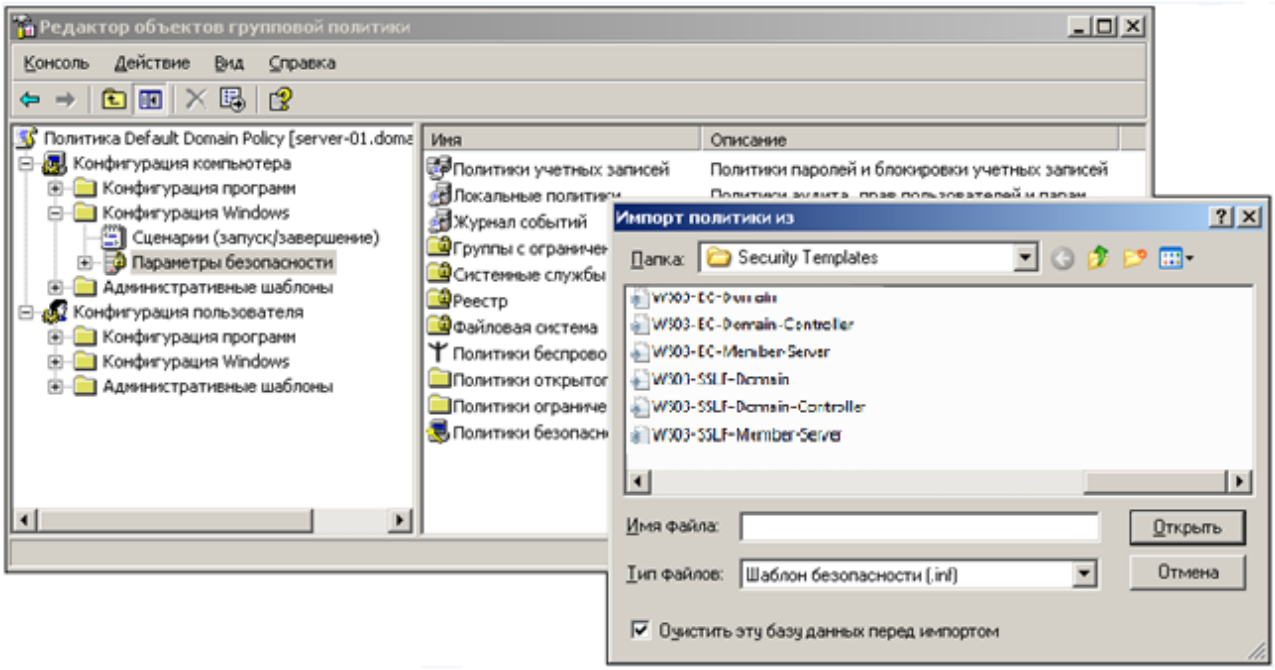


Рисунок 2.11

7. Закрыть редактор объектов групповой политики.

8. В командной строке выполнить команду `gpudate.exe /force`, позволяющую осуществить принудительную репликацию и обновление измененной политики безопасности контроллерами домена (см. рисунок 2.12).

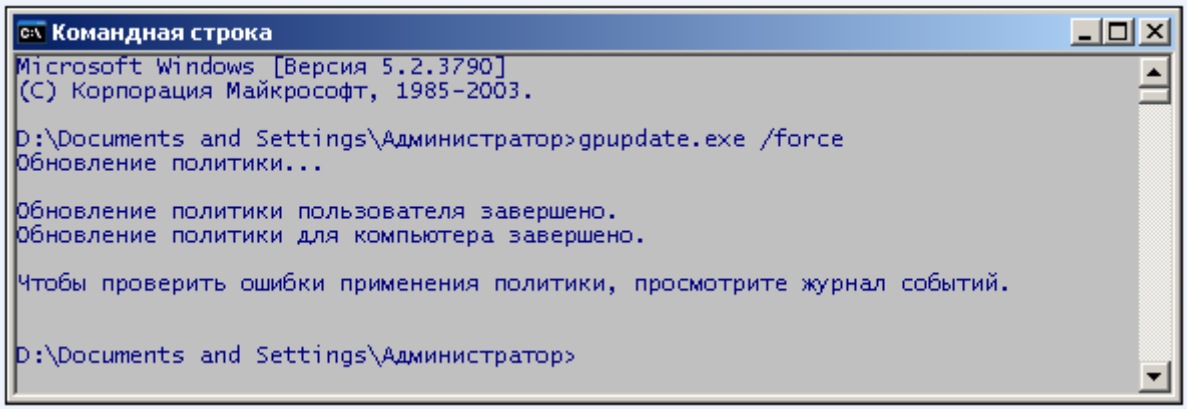


Рисунок 2.12

9. Проанализировать журнал регистрации событий «Приложение» на предмет наличия ошибок, которые могли возникнуть на этапе репликации или обновления политики безопасности. В случае успешного применения политики безопасности в объекте групповой политики в журнале «Приложение» должно быть зарегистрировано событие с кодом `ID:1704` (см. рисунок 2.13).

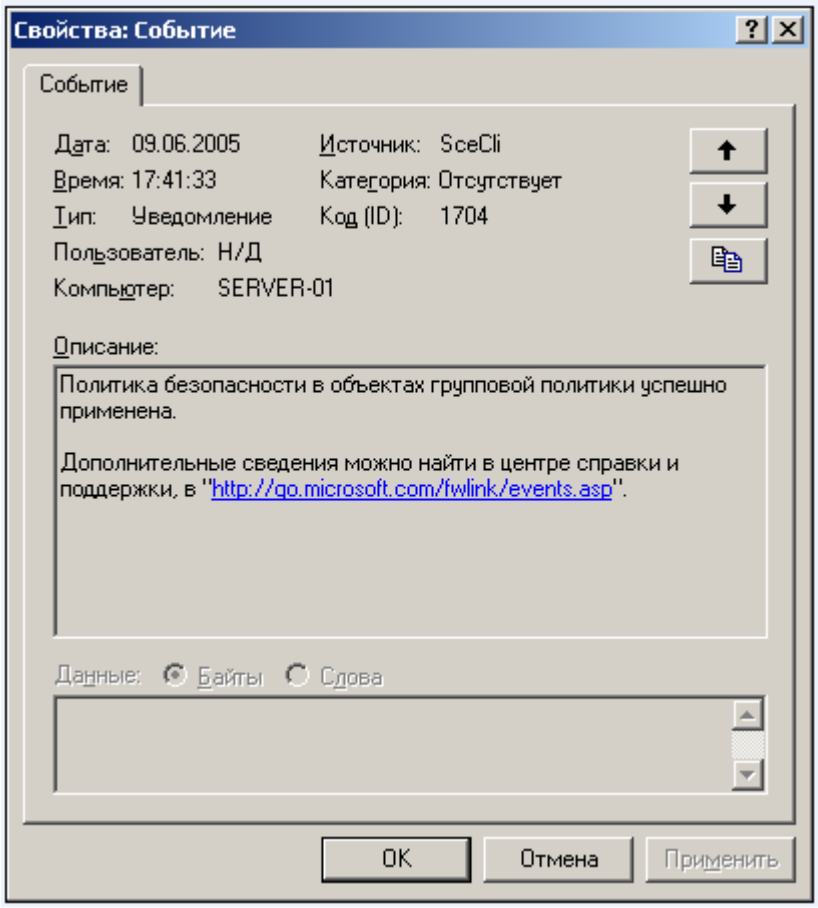


Рисунок 2.13

При назначении политики учетных записей на уровне домена необходимо убедиться, что в списке управления доступом ACL соответствующего объекта групповой политики для пользователей и компьютеров домена определены разрешения «Чтение» и «Применение групповой политики». Если в списке управления доступом не будут определены требуемые значения, политика учетных записей к указанным субъектам применена не будет.

Кроме того, для объекта групповой политики должен быть применен параметр принудительного наследования «Не перекрывать: другие объекты групповой политики не могут перекрывать параметры этой политики», позволяющий применять групповую политику ко всем пользователям и компьютерам независимо от того, где они расположены, и обеспечивающий невозможность перекрытия параметров данного ОГП параметрами других ОГП (см. рисунок 2.14).

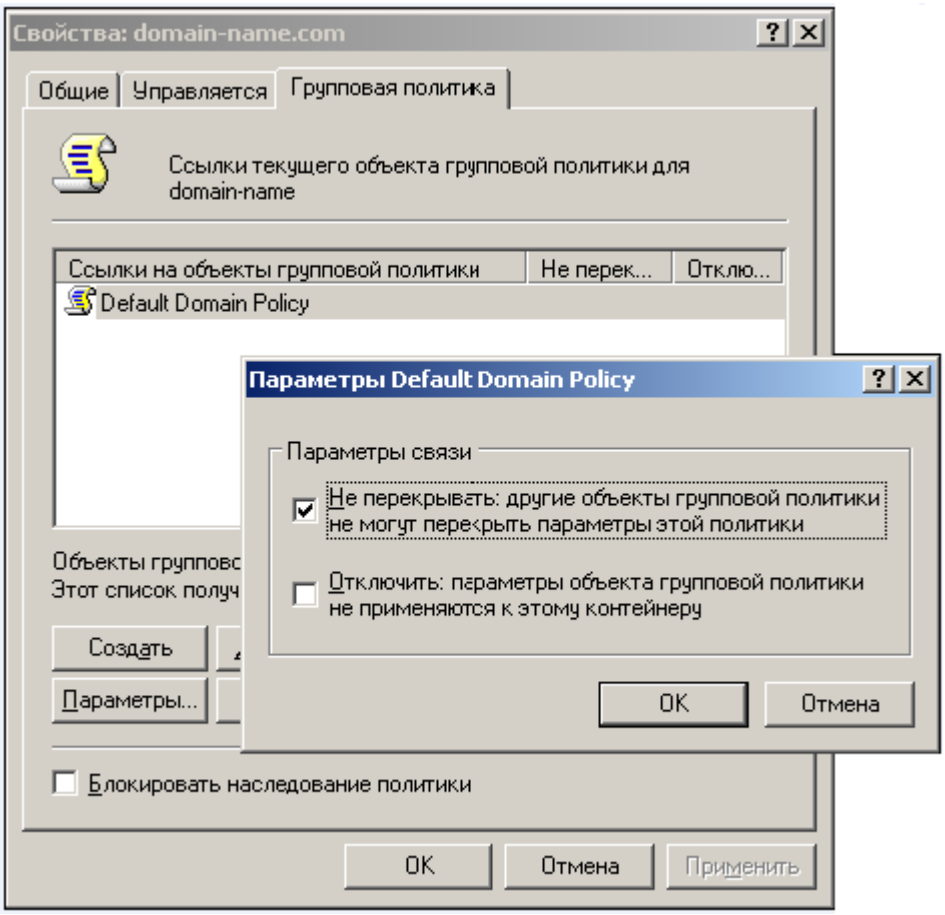


Рисунок 2.14

Чтобы применить единые параметры безопасности для всех рядовых серверов домена необходимо:

1. Создать с использованием «Мастера настройки безопасности» политику безопасности, включающую в себя шаблон безопасности WS03-EC-Member-Server.inf (порядок создания политики описан в пп.2.3.1).

2. Преобразовать с использованием утилиты командной строки `Scwcmd.exe` созданную политику безопасности в объект групповой политики (порядок использования утилиты описан в пп.2.3.2).

3. Привязать созданный объект групповой политики к организационному подразделению, содержащему учетные записи рядовых серверов домена под управлением ОС Microsoft® Windows Servertм 2003 , реализующих предопределенные роли.

Чтобы привязать объект групповой политики к соответствующему организационному подразделению необходимо выполнить следующие действия:

1. Нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду `dsa.msc` и нажать «ОК».

2. В появившемся окне оснастки консоли управления «Active Directory –

пользователи и компьютеры» выделить имя организационного подразделения (например, `Member Servers`) и посредством пункта «Свойства» контекстного меню получить доступ к диалоговому окну свойств указанного ОП. Далее перейти на вкладку «Групповая политика».

3. Привязать объект групповой политики к соответствующему организационному подразделению. Для этого в окне свойств соответствующего организационного подразделения на вкладке «Групповая политика» нажать «Добавить», в появившемся диалоговом окне добавления ссылки на ОГП перейти на вкладку «Все» и выбрать соответствующий объект групповой политики (см. рисунок 2.15).

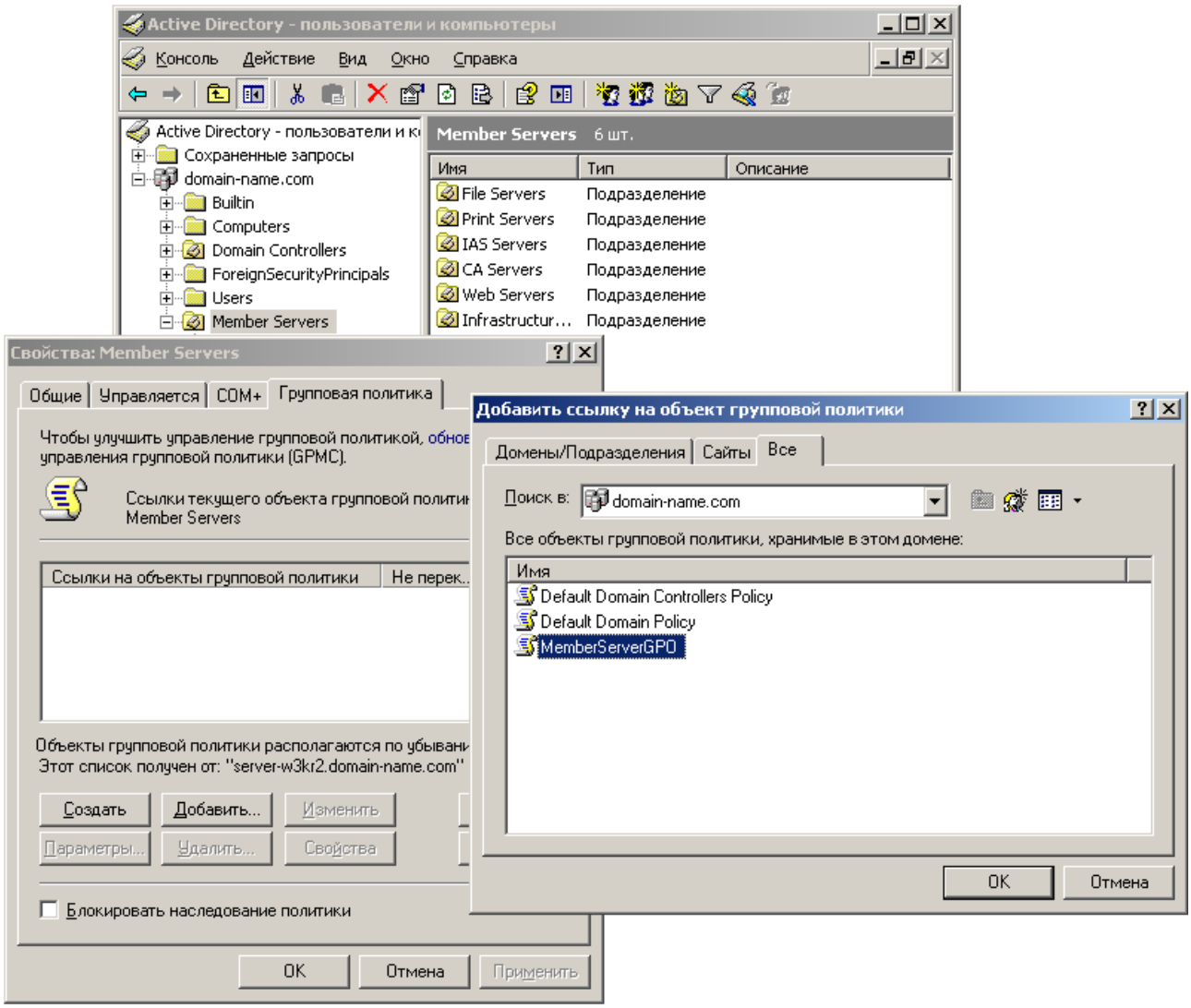


Рисунок 2.15

Для указанного объекта групповой политики должен быть применен параметр принудительного наследования «`Не перекрывать: другие объекты групповой политики не могут перекрывать параметры этой политики`», что не позволит ОГП, определяемых на более низких уровнях иерархии ОП, переопределять заданные данной

групповой политикой параметры безопасности.

4. В командной строке выполнить команду `gpudate.exe /force`, позволяющую осуществить принудительную репликацию и обновление измененной политики безопасности контроллерами домена.

5. Проанализировать журнал регистрации событий «Приложение» на предмет наличия ошибок, которые могли возникнуть на этапе репликации или обновления политики безопасности. В случае успешного применения политики безопасности в объекте групповой политики в журнале «Приложение» должно быть зарегистрировано событие с кодом `ID:1704`.

Применение единых параметров безопасности для рядовых серверов под управлением ОС Microsoft® Windows Servertм 2003 , реализующих конкретную роль, также необходимо осуществлять путем создания отдельных политик безопасности, учитывающих специфичные для конкретной роли рядового сервера параметры безопасности (соответствие между реализуемой компьютером ролью и включаемым в политику шаблоном безопасности представлено в таблице 2.2), последующего их преобразования с помощью утилиты командной строки `Scwcmd.exe` в объекты групповой политики и привязки полученных ОГП к соответствующим организационном подразделениям, содержащим учетные записи данных компьютеров.

Все действия по созданию политики безопасности с использованием «Мастера настройки безопасности» описаны в пп.2.3.1 настоящего руководства, порядок привязки созданных ОГП к соответствующему организационному подразделению аналогичен той же последовательности действий, которая описана выше.

2.5 Настройка компьютера, являющегося членом домена Active Directory, в конфигурации «Specialized Security – Limited Functionality»

2.5.1 Используемые шаблоны безопасности

Для автоматической настройки параметров политики учетных записей следует импортировать шаблон безопасности `WS03-SSLF-Domain.inf` в требуемый объект групповой политики, определяемый на уровне домена (в частности, в ОГП «Default Domain Policy» - политика домена, используемая по умолчанию), на контроллере домена под управлением операционной системы Microsoft® Windows Server 2003™.

Для настройки общих для всех рядовых серверов в рамках домена параметров безопасности необходимо с использованием «Мастера настройки безопасности» создать

соответствующую политику (см. пп.2.3.1 настоящего Руководства), учитывающей требуемые аспекты безопасности, и включить в нее шаблон безопасности WS03-SSLF-Member-Server.inf. Далее с использованием утилиты командной строки `Scwcmd.exe` преобразовать полученную политику в соответствующий объект групповой политики и осуществить его привязку к организационному подразделению, содержащему учетные записи всех рядовых серверов домена (ОП «Member Servers»), реализующих предопределенные роли (см. рисунок 2.1).

Для настройки параметров безопасности, учитывающих особенности, связанные с выполнением компьютером определенной роли, необходимо с использованием «Мастера настройки безопасности» дополнительно создать соответствующую политику безопасности, включив в нее требуемый шаблон безопасности (см. таблицу 2.3). Далее с использованием утилиты командной строки `Scwcmd.exe` преобразовать полученную политику в ОГП и осуществить его привязку к организационному подразделению, содержащему учетные записи компьютеров, реализующих одинаковую роль. Соответствие между реализуемыми компьютером под управлением ОС Microsoft® Windows Servertм 2003 в конфигурации «Enterprise Client» ролями и включаемыми в политики безопасности шаблонами представлено в таблице 2.3.

Таблица 2.3 - Соответствие возможных вариантов функционирования ОС Microsoft® Windows Servertм 2003 в конфигурации «Enterprise Client» и применяемых шаблонов безопасности

№ п/п	Роли, реализуемые ОО	Применяемые шаблоны безопасности
1.	Контроллер домена	WS03-SSLF-Domain-Controller.inf
2.	Сервер служб сетевой инфраструктуры	WS03-SSLF-Member-Server.inf
3.	Файловый сервер	
4.	Сервер печати	
5.	Сервер служб Интернета	

2.5.2 Порядок применения шаблонов безопасности и объектов групповой политики

Импорт шаблона безопасности WS03-SSLF-Domain.inf необходимо осуществлять с использованием редактора соответствующего объекта групповой политики, определяемого

на уровне домена (например, ОГП «Default Domain Policy»). Чтобы импортировать шаблон безопасности в соответствующий ОГП необходимо выполнить следующие действия:

1. Нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду `dsa.msc` и нажать «ОК».

2. В появившемся окне оснастки консоли управления «Active Directory – пользователи и компьютеры» выделить имя домена (например, `domain-name.com`) и посредством пункта «Свойства» контекстного меню получить доступ к диалоговому окну свойств существующего домена. Далее, перейти на вкладку «Групповая политика» (см. рисунок 2.16).

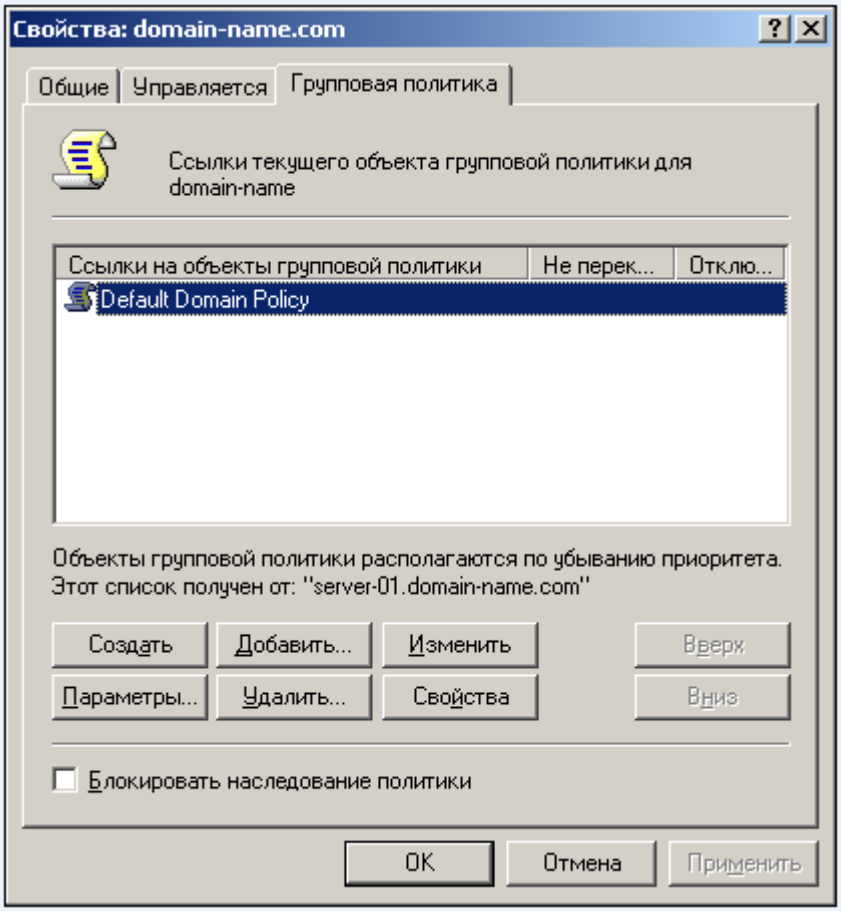


Рисунок 2.16

3. Вызвать редактор объектов групповой политики (Group Policy Object Editor). Для этого необходимо выбрать требуемый объект групповой политики, определяемый на уровне домена, (в частности, ОГП «Default Domain Policy») и нажать «Изменить». В случае, если существует необходимость, администратором на уровне домена может быть создан новый объект групповой политики с привязкой к указанному домену. Для этого в окне свойств существующего домена на вкладке «Групповая политика» следует нажать «Создать» и ввести имя нового объекта групповой политики.

4. В окне редактора объектов групповой политики выбрать узел «Конфигурация компьютера» и перейти к разделу «Конфигурация Windows».

5. Выделить папку «Параметры безопасности» и посредством контекстного меню выбрать пункт «Импорт политики».

6. В появившемся диалоговом окне импорта политики выбрать шаблон безопасности WS03-SSLF-Domain.inf, и нажать кнопку «Открыть». После чего параметры безопасности импортируются из выбранного файла в текущий объект групповой политики (см. рисунок 2.17).

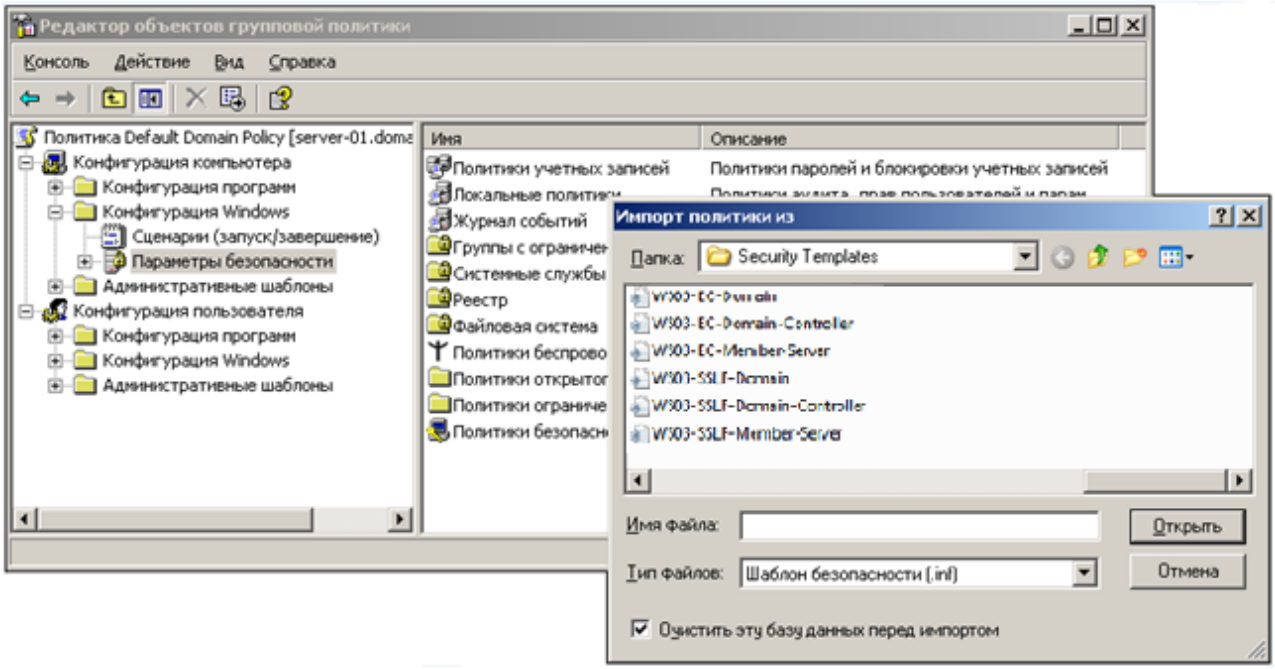


Рисунок 2.17

7. Закрыть редактор объектов групповой политики.

8. В командной строке выполнить команду `gpudate.exe /force`, позволяющую осуществить принудительную репликацию и обновление измененной политики безопасности контроллерами домена (см. рисунок 2.18).

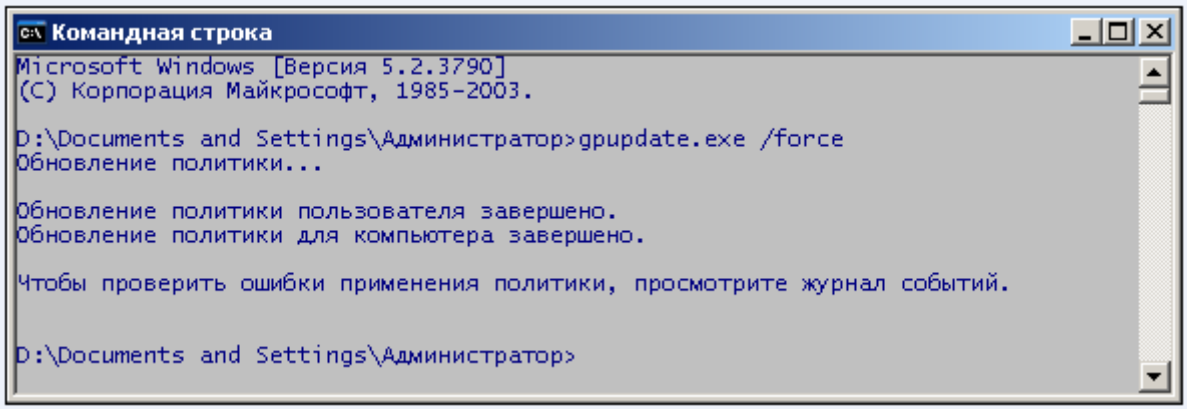


Рисунок 2.18

9. Проанализировать журнал регистрации событий «Приложение» на предмет наличия ошибок, которые могли возникнуть на этапе репликации или обновления политики безопасности. В случае успешного применения политики безопасности в объекте групповой политики в журнале «Приложение» должно быть зарегистрировано событие с кодом `ID:1704` (см. рисунок 2.19).

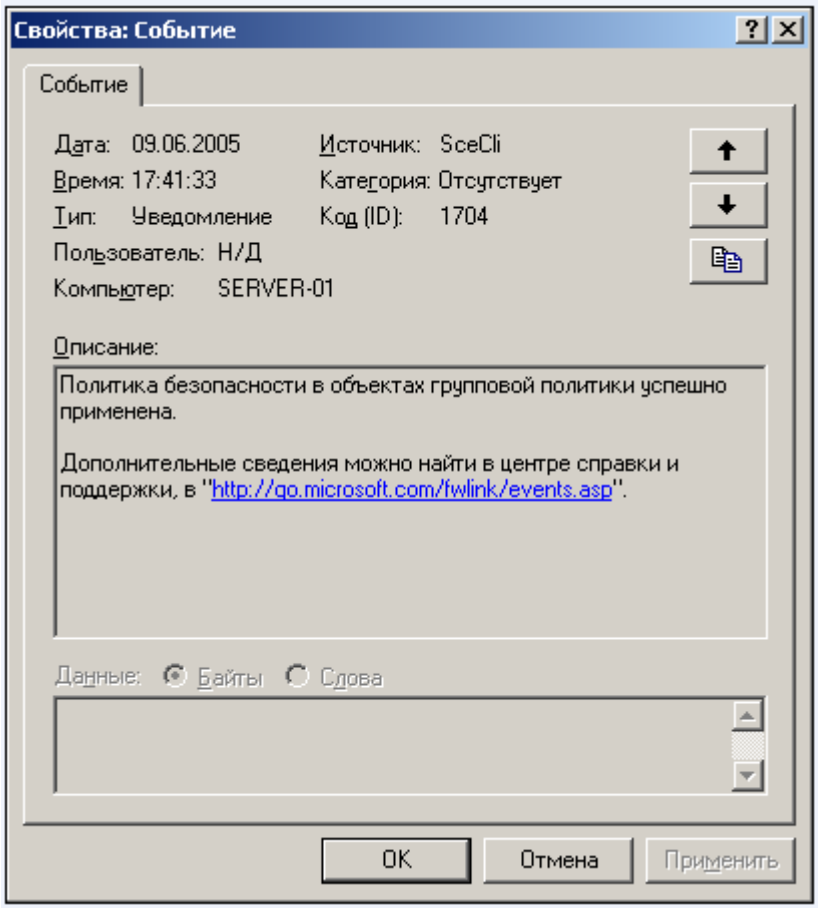


Рисунок 2.19

При назначении политики учетных записей на уровне домена необходимо убедиться, что в списке управления доступом ACL соответствующего объекта групповой политики для пользователей и компьютеров домена определены разрешения «Чтение» и «Применение групповой политики». Если в списке управления доступом не будут определены требуемые значения, политика учетных записей к указанным субъектам применена не будет.

Кроме того, для объекта групповой политики должен быть применен параметр принудительного наследования «Не перекрывать: другие объекты групповой политики не могут перекрывать параметры этой политики», позволяющий применять групповую политику ко всем пользователям и компьютерам независимо от того, где они расположены, и обеспечивающий невозможность перекрытия параметров данного ОГП параметрами других ОГП (см. рисунок 2.20).

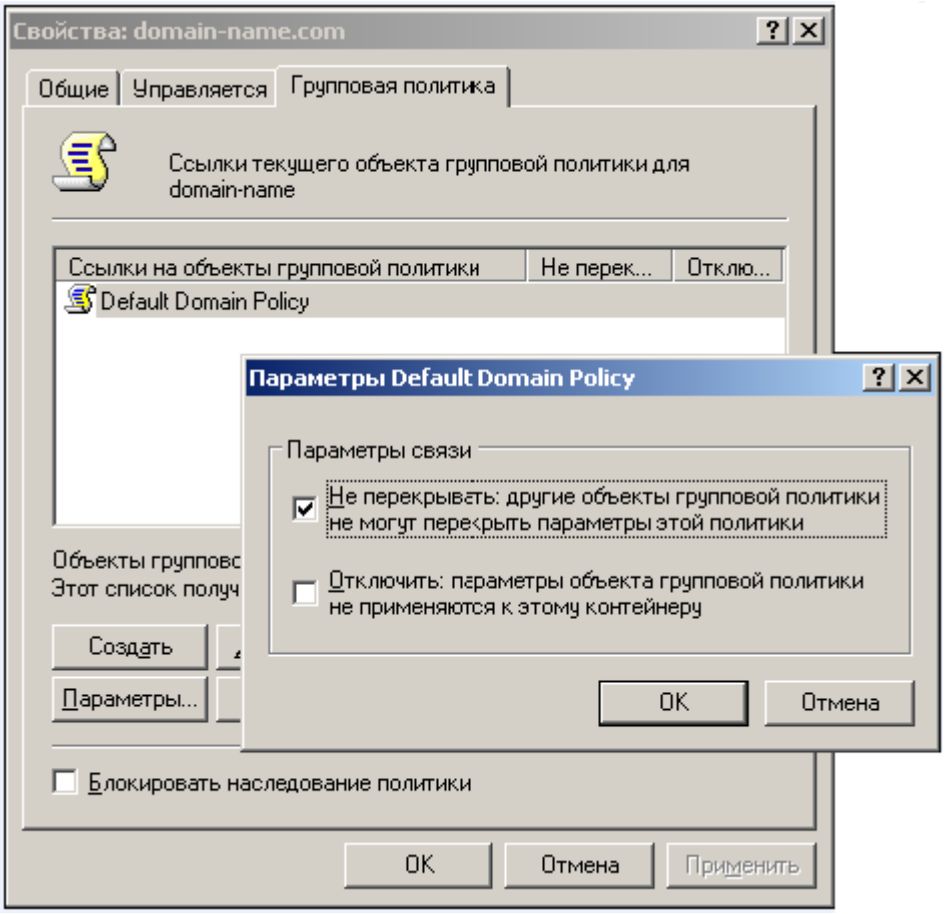


Рисунок 2.20

Чтобы применить единые параметры безопасности для всех рядовых серверов домена необходимо:

1. Создать с использованием «Мастера настройки безопасности» политику безопасности, включающую в себя шаблон безопасности WS03-SSLF-Member-Server.inf (порядок создания политики описан в пп.2.3.1).

2. Преобразовать с использованием утилиты командной строки `Scwcmd.exe` созданную политику безопасности в объект групповой политики (порядок использования утилиты описан в пп.2.3.2).

3. Привязать созданный объект групповой политики к организационному подразделению, содержащему учетные записи рядовых серверов домена под управлением ОС Microsoft® Windows Servertм 2003 , реализующих предопределенные роли.

Чтобы привязать объект групповой политики к соответствующему организационному подразделению необходимо выполнить следующие действия:

1. Нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду `dsa.msc` и нажать «ОК».

2. В появившемся окне оснастки консоли управления «Active Directory – пользователи и компьютеры» выделить имя организационного подразделения (например, `Member Servers`) и посредством пункта «Свойства» контекстного меню получить доступ к диалоговому окну свойств указанного ОП. Далее перейти на вкладку «Групповая политика».

3. Привязать объект групповой политики к соответствующему организационному подразделению. Для этого в окне свойств соответствующего организационного подразделения на вкладке «Групповая политика» нажать «Добавить», в появившемся диалоговом окне добавления ссылки на ОГП перейти на вкладку «Все» и выбрать соответствующий объект групповой политики (см. рисунок 2.21).

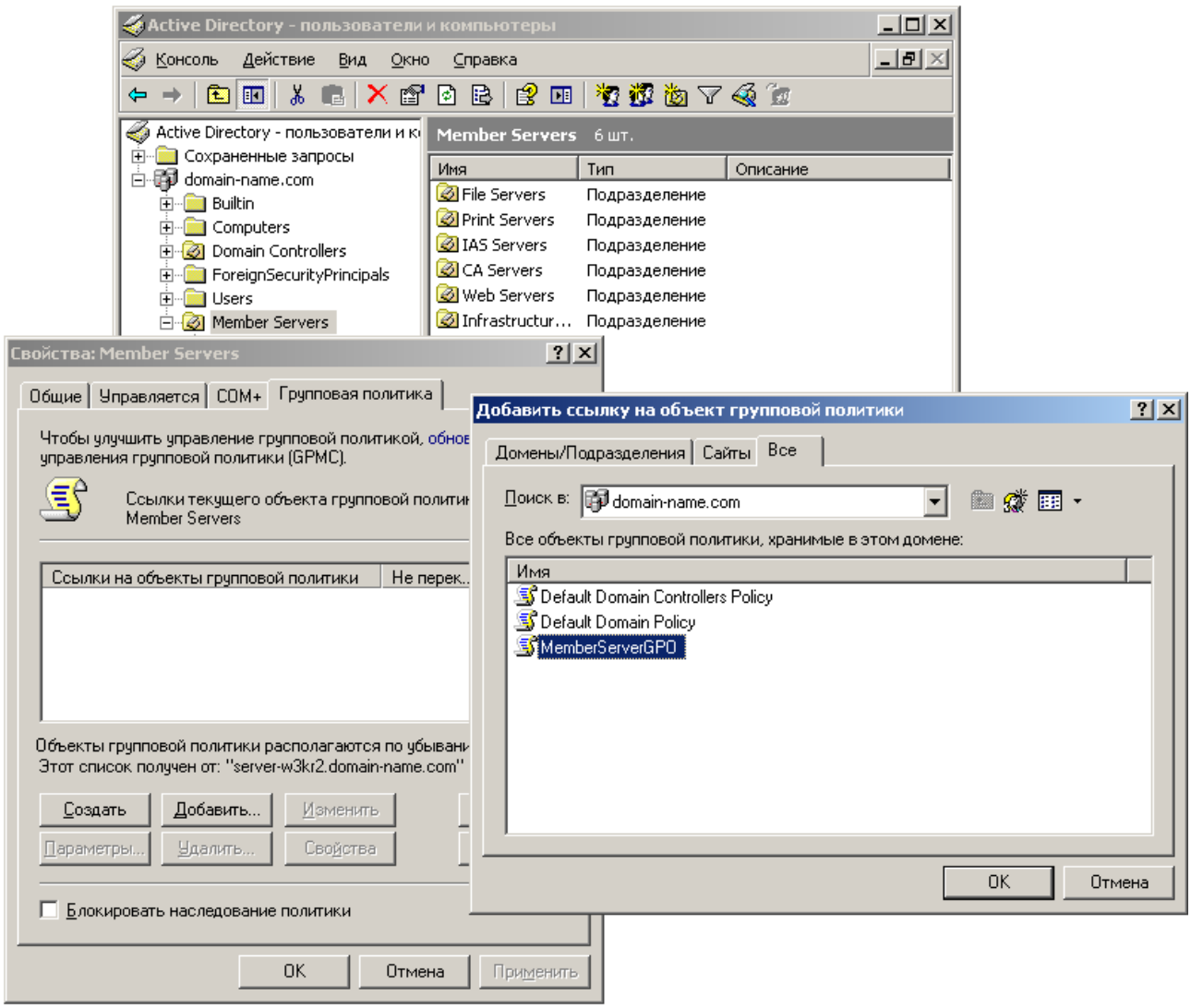


Рисунок 2.21

Для указанного объекта групповой политики должен быть применен параметр принудительного наследования «`Не перекрывать: другие объекты групповой политики не могут перекрывать параметры этой политики`», что не позволит ОГП, определяемых на более низких уровнях иерархии ОП, переопределять заданные данной групповой политикой параметры безопасности.

4. В командной строке выполнить команду `gpudate.exe /force`, позволяющую осуществить принудительную репликацию и обновление измененной политики безопасности контроллерами домена.

5. Проанализировать журнал регистрации событий «Приложение» на предмет наличия ошибок, которые могли возникнуть на этапе репликации или обновления политики безопасности. В случае успешного применения политики безопасности в объекте групповой

политики в журнале «Приложение» должно быть зарегистрировано событие с кодом `ID:1704`.

Применение единых параметров безопасности для рядовых серверов под управлением ОС Microsoft® Windows Servertм 2003 , реализующих конкретную роль, также необходимо осуществлять путем создания отдельных политик безопасности, учитывающих специфичные для конкретной роли рядового сервера параметры безопасности (соответствие между реализуемой компьютером ролью и включаемым в политику шаблоном безопасности представлено в таблице 2.3), последующего их преобразования с помощью утилиты командной строки `Scwcmd.exe` в объекты групповой политики и привязки полученных ОГП к соответствующим организационном подразделениям, содержащим учетные записи данных компьютеров.

Все действия по созданию политики безопасности с использованием «Мастера настройки безопасности» описаны в пп.2.3.1 настоящего руководства, порядок привязки созданных ОГП к соответствующему организационному подразделению аналогичен той же последовательности действий, которая описана выше.

2.6 Настройка автономного компьютера под управлением ОС Microsoft® Windows Server™ 2003, выступающего в роли бастион-хоста

2.6.1 Используемые шаблоны безопасности

С целью обеспечения требуемого уровня безопасности, необходимого для обработки конфиденциальной информации, автономные компьютеры под управление операционной системы Microsoft® Windows Servertм 2003 , выступающие в роли бастион-хоста, должны быть настроены в конфигурации «Specialized Security – Limited Functionality». Для приведения указанных компьютеров в соответствующую конфигурацию, администратор должен обеспечить применение параметров безопасности, определенные в шаблоне WS03-SSLF-Bastion-Host.inf, к локальной политике безопасности.

Настройка параметров безопасности автономного компьютера, выступающего в роли бастион-хоста, может быть осуществлена следующими способами:

- с использованием инструментария «Мастер настройки безопасности»;
- с использованием консоли управления «Анализ и настройка безопасности»;
- с использованием инструментального средства командной строки `Secedit.exe`.

2.6.2 Порядок настройки компьютера, выступающего в роли бастион-хоста

Настройка с использованием инструментария «Мастер настройки безопасности»

Порядок настройки компьютера, выступающего в роли бастион-хоста, с использованием «Мастера настройки безопасности аналогичен порядку, описанному в пп.2.3.1 настоящего руководства, за исключением шагов 13-14.

На странице задания имени файла политики безопасности администратору следует включить в создаваемую политику шаблон безопасности WS03-SSLF-Bastion-Host.inf.

На странице выбора вариантов применения созданной политики безопасности выбрать опцию «Применить сейчас» и нажать «Далее». После нажатия «Далее» мастер применит созданную администратором политику безопасности к локальному компьютеру, выступающему в роли бастион-хоста.

Настройка с использование консоли управления «Анализ и настройка безопасности»

Настройка компьютера, выступающего в роли бастион-хоста, в конфигурации безопасности «Specialized Security – Limited Functionality» предусматривает импортирование шаблона безопасности WS03-SSLF-Bastion-Host.inf в локальный объект групповой политики.

Для импортирования шаблона безопасности WS03-SSLF-Bastion-Host.inf необходимо выполнить следующие действия:

1. Открыть оснастку консоли управления «Анализ и настройка безопасности». Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду `mmc` и нажать «ОК». В окне консоли управления MMC (Microsoft Management Console) посредством пункта меню «Добавить или удалить оснастку…» добавить изолированную оснастку «Анализ и настройка безопасности» (см. рисунок 2.28).

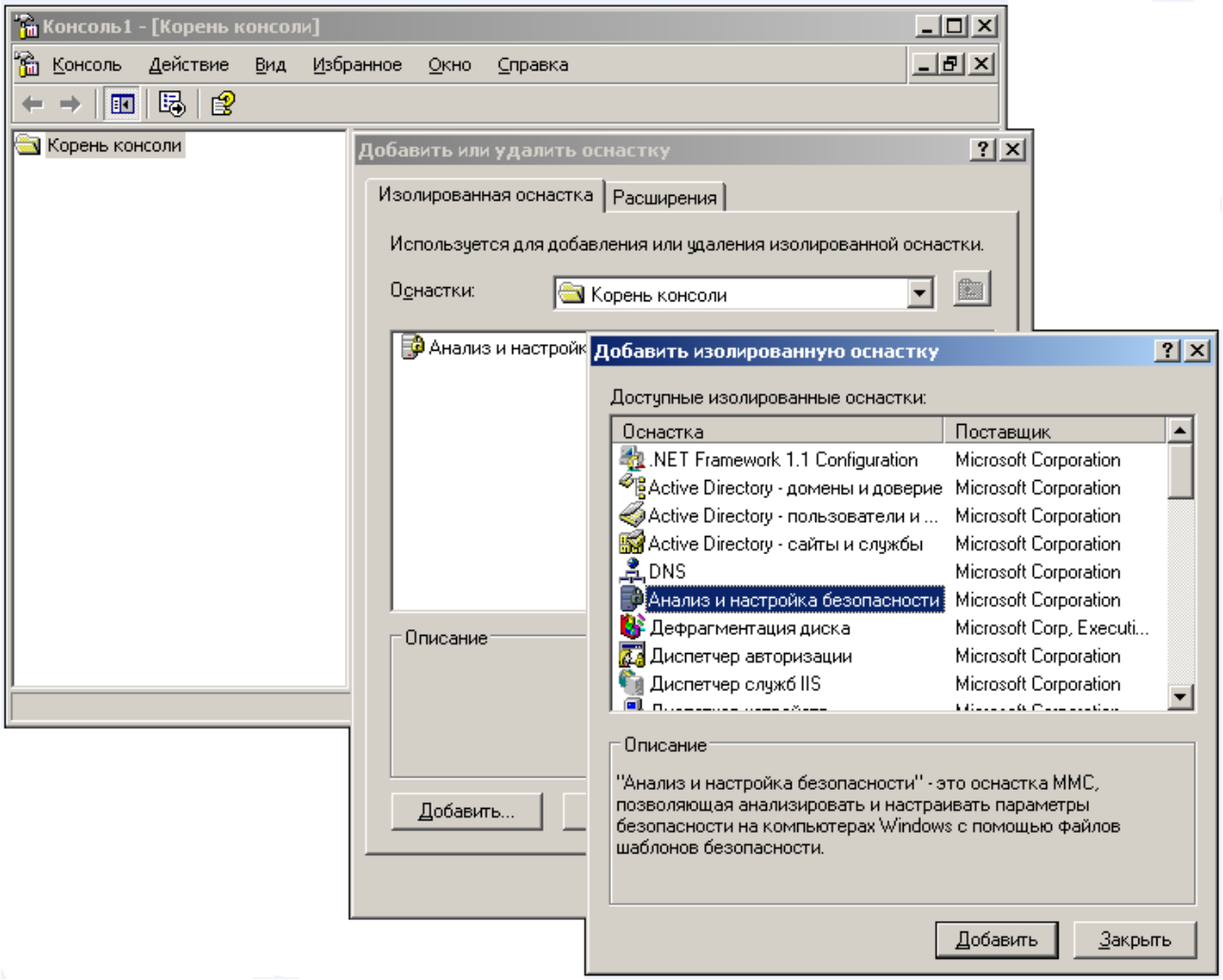


Рисунок 2.28

2. В дереве консоли посредством нажатия правой кнопкой мыши узла «Анализ и настройка безопасности» выбрать команду «Открыть базу данных».

3. В диалоговом окне «Открыть базу данных» выполнить одно из следующих действий (см. рисунок 2.24):

– создать новую базу данных анализа. Для этого необходимо ввести новое имя в поле «Имя файла» и нажать «Открыть». При открытии новой базы данных в диалоговом окне «Импорт шаблона» выбрать импортируемый шаблон безопасности WS03-SSLF-Bastion-Host.inf и нажать кнопку «Открыть»;

– открыть существующую базу данных анализа. Для этого необходимо выделить имя базы данных и нажать «Открыть».

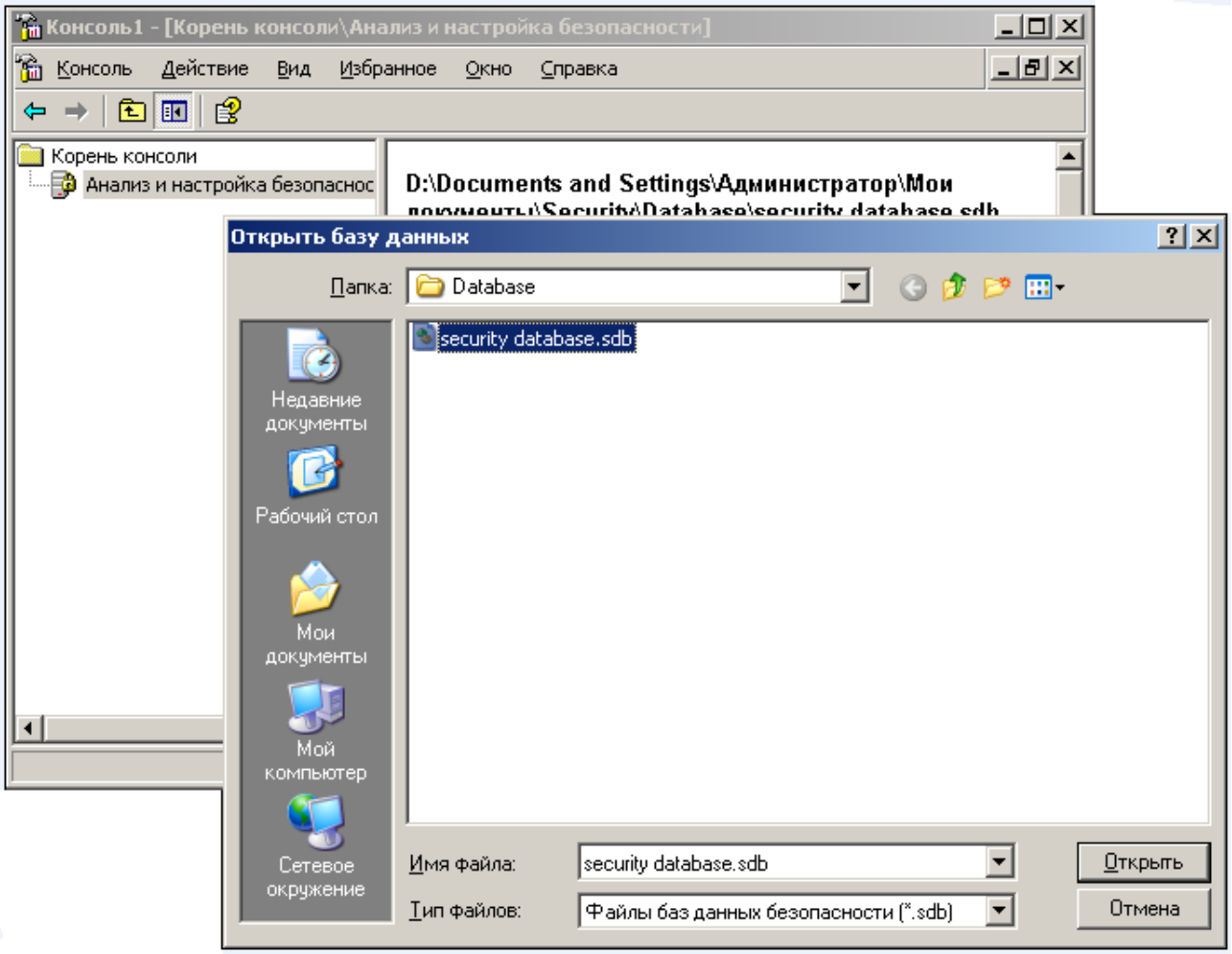


Рисунок 2.29

4. Импортировать шаблон безопасности WS03-SSLF-Bastion-Host.inf, определяющий требуемые параметры политики безопасности. Для этого в диалоговом окне консоли «Анализ и настройка безопасности» выбрать пункт меню «Действие» и далее «Импорт шаблона». При импортировании шаблона безопасности администратором должны быть учтены следующие аспекты:

– в случае использования существующей базы данных анализа и импортирования в нее нового шаблона безопасности в диалоговом окне «Импорт шаблона» необходимо выбрать опцию «Очистить эту базу данных перед импортом», что приведет к перезаписи всех шаблонов, хранящихся в базе данных, импортируемым шаблоном. Если данная опция снята, импортируемый шаблон безопасности будет объединен с сохраненными шаблонами, и в базе данных будет храниться составной шаблон безопасности;

– в случае использования новой базы данных при импортировании шаблона безопасности опция «Очистить эту базу данных перед импортом» может быть отключена.

5. Посредством нажатия правой кнопкой мыши узла «Анализ и настройка безопасности» выбрать команду «Настроить компьютер» (см. рисунок 2.30).

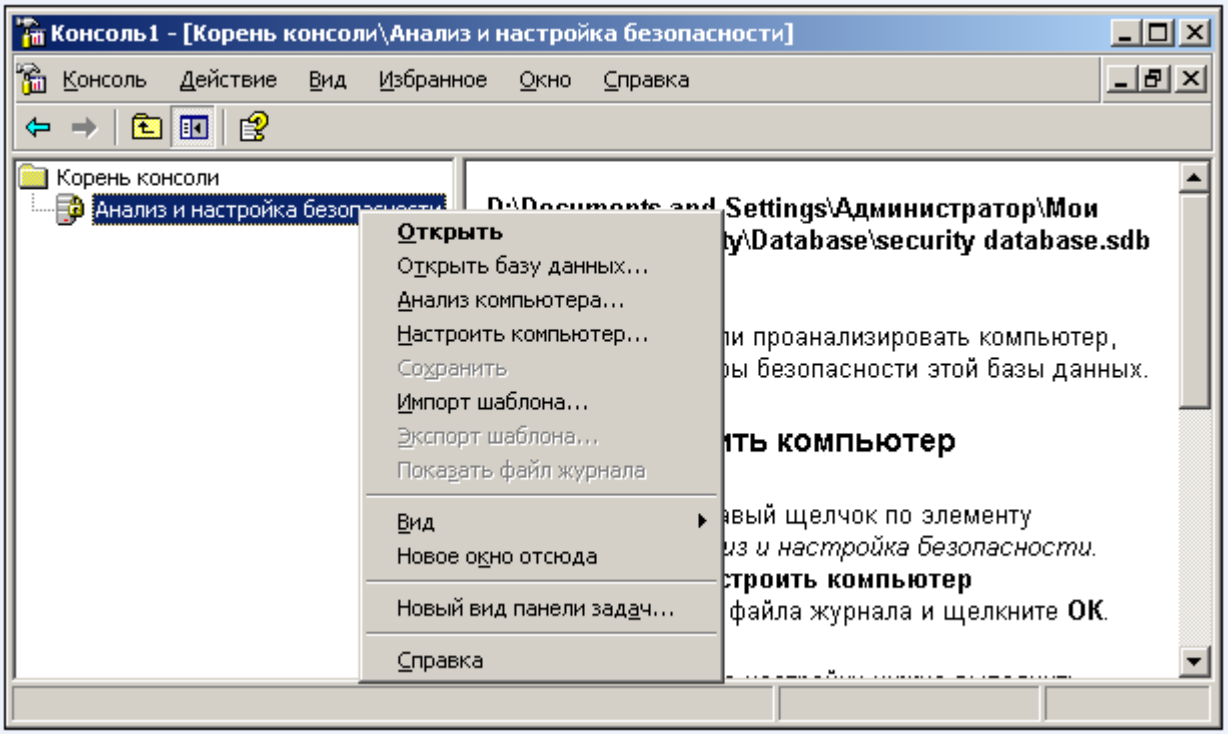


Рисунок 2.30

6. Проанализировать содержимое журнала регистрации событий на предмет наличия ошибок, возникших на этапе применение шаблона безопасности к локальной политики безопасности (см. рисунок 2.31).

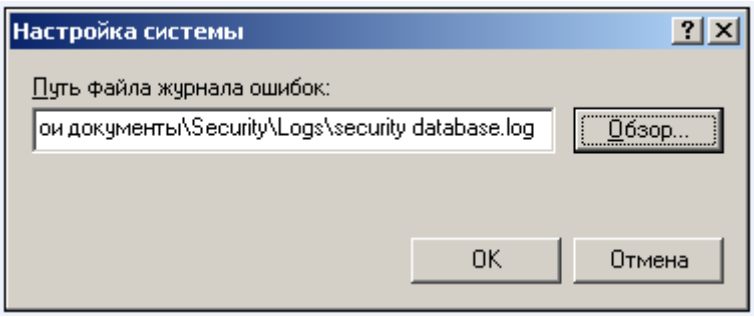


Рисунок 2.31

7. Закрыть оснастку «Анализ и настройка безопасности».

2.7 Порядок отключения функции автоматического обновления операционной системы Microsoft® Windows Servertм 2003

Одним из основных условий соответствия сертифицированной версии операционной системы Microsoft® Windows Servertм 2003 является наличие полного набора сертифицированных обновлений безопасности.

Чтобы исключить автоматическую загрузку и установку обновлений, доступных на веб-узле Windows Update, и обеспечить копирование только рекомендованных и обязательных к установке сертифицированных наборов исправлений безопасности или пакетов обновлений, доступных в Центре цертифициованных обновлений на защищенном разделе сайта «http://www.altx-soft.ru/downloads.htm», необходимо отключить функцию автоматического обновления операционной системы Microsoft® Windows Servertм 2003 . В результате система не будет осуществлять автоматическую установку доступных обновлений, а пользователь, в свою очередь, будет контролировать весь процесс загрузки и установки обновлений.

Для отключения функции автоматического обновления операционной системы Microsoft® Windows Servertм 2003 необходимо выполнить следующие действия:

1. Отключить компонент системы «Автоматическое обновление»:
   - осуществить вход в систему с использованием учетной записи администратора;
   - нажать кнопку «Пуск», выбрать пункт меню «Панель управления» и далее «Система»;
   - перейти на вкладку «Автоматическое обновление»;
   - отключить опцию «Выполнять обновление системы» (см. рисунок 2.33).

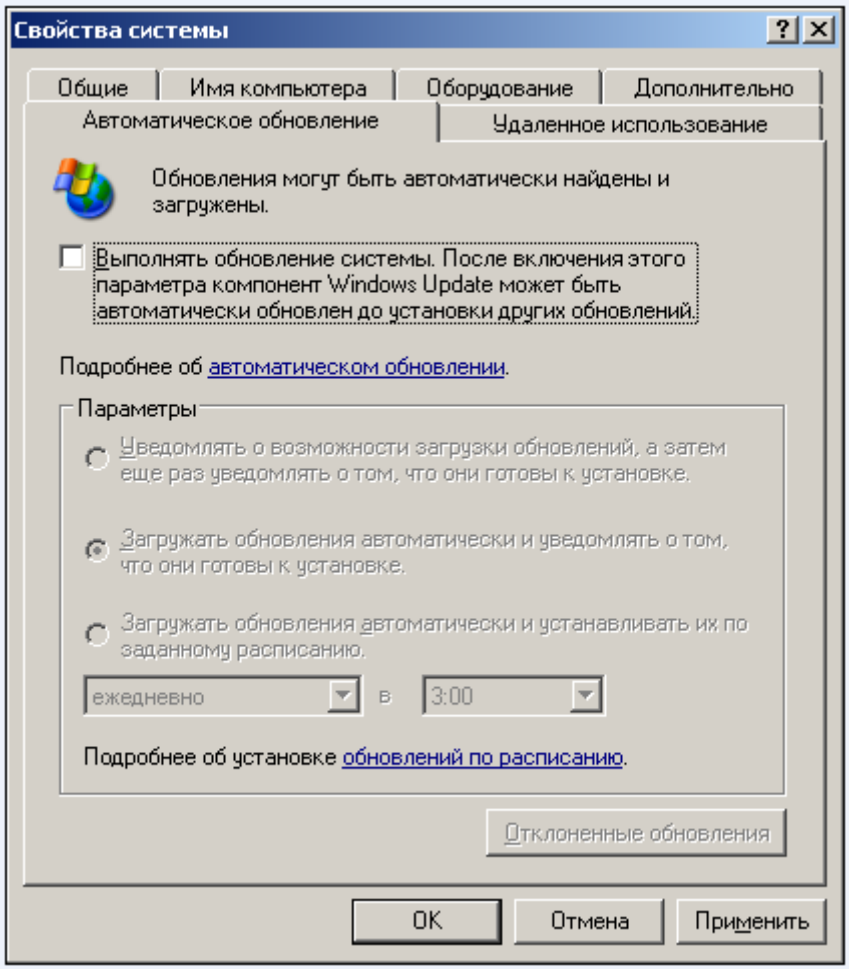


Рисунок 2.33

– нажать «ОК» для принятия изменений и закрытия диалогового окна «Свойства системы».

2. Выполнить программный останов службы «Автоматическое обновление»:
   – вызвать оснастку «Службы» консоли управления Microsoft. Для этого нажать кнопку «Пуск» и выбрать пункт меню «Панель управления»;
   – в диалоговом окне «Панель управления» выбрать значок панели администрирования «Администрирование» и далее пункт «Службы»;
   – в диалоговом окне консоли управления «Службы» выбрать службу «Автоматическое обновление» и посредством пункта «Свойства» контекстного меню вызвать окно свойств службы «Автоматическое обновление» (см. рисунок 2.34);

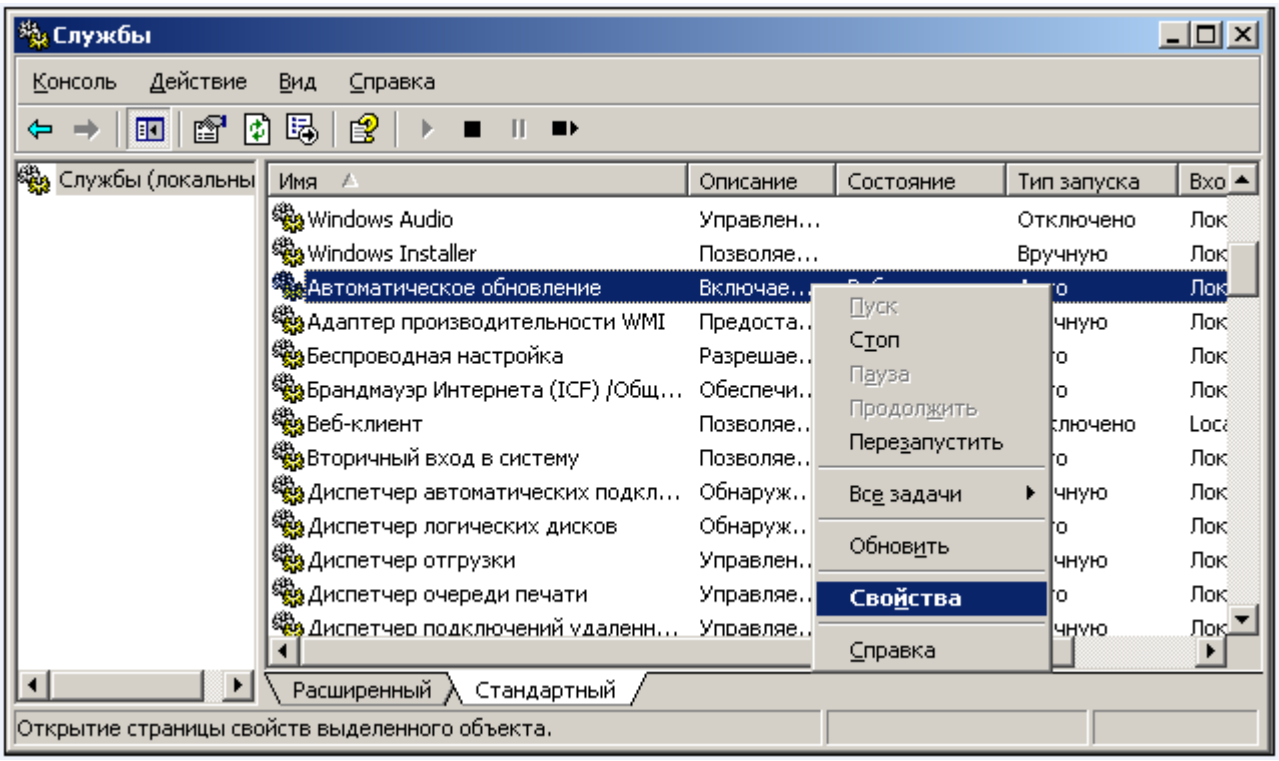


Рисунок 2.34

– в окне свойств службы «Автоматическое обновление» изменить тип запуска на «Отключено» и посредством нажатия кнопки «Стоп» остановить работу службы (см. рисунок 2.35);

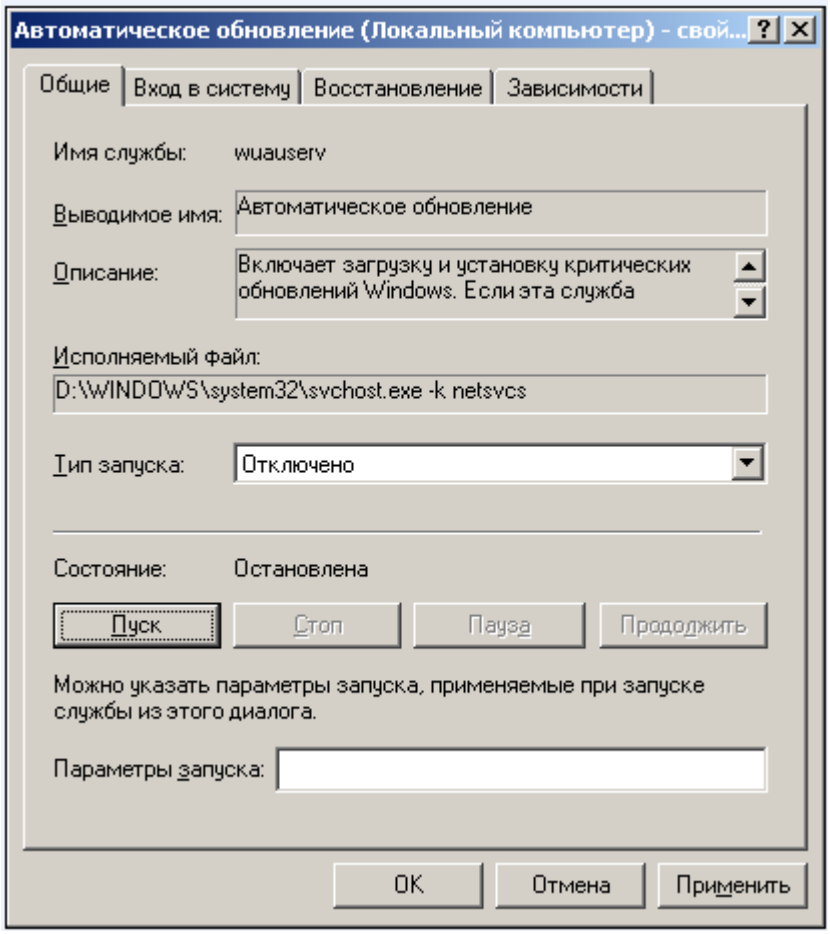


Рисунок 2.35

– нажать «ОК» для принятия изменений и закрытия диалогового окна свойств службы «Автоматическое обновление»;
– закрыть диалоговое окно оснастки консоли управления «Службы».

Кроме того, отключение функции автоматического обновления операционной системы Microsoft® Windows Servertм 2003 может быть осуществлено с использованием локальной или доменной групповых политик.

Для отключения компонента «Автоматическое обновление» с помощью локальной групповой политики необходимо выполнить следующие действия:

– осуществить вход в систему с использованием учетной записи администратора;
– нажать кнопку «Пуск» и выбрать пункт «Выполнить…»;
– в поле «Открыть» диалогового окна «Запуск программы» набрать команду `gpedit.msc` и нажать «ОК»;
– в окне редактора локальной групповой политики «Локальный компьютер» выбрать узел «Конфигурация компьютера» и перейти к разделу «Административные шаблоны»;

– правой кнопкой мыши нажать на элемент «Административные шаблоны» и в появившемся окне контекстного меню выбрать команду «Добавление и удаление шаблонов»;
– нажать кнопку «Добавить», в открывшемся диалоговом окне выбора шаблонов политик выбрать файл административного шаблона `Wuau.adm`, расположенный в папке `%SystemRoot%\Inf`, и нажать «Открыть» (см. рисунок 2.36);

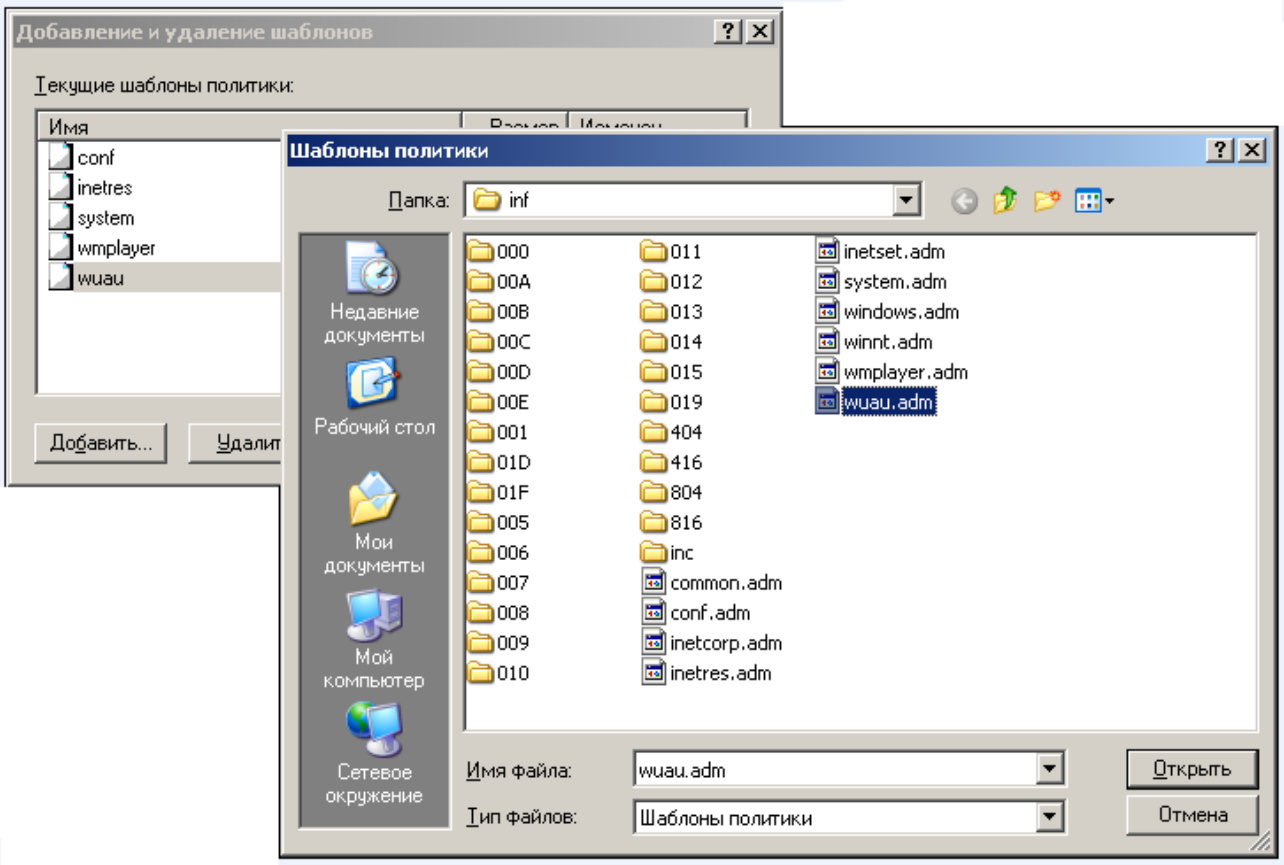


Рисунок 2.36

– нажать кнопку «Закрыть»;
– в дереве «Конфигурация компьютера» последовательно развернуть узлы «Административные шаблоны», «Компоненты Windows» и «Windows Update» и перейти к политике «`Настройка автоматического обновления`», в которой указано, использует ли компьютер службу автоматического обновления операционной системы Microsoft® Windows Servertм 2003 для получения обновлений безопасности и других исправлений. Параметры данной политики предназначены для настройки службы автоматического обновления операционной системы;

– посредством двойного нажатия открыть диалоговое окно свойств политики «Настройка автоматического обновления»;
– на вкладке «Параметр» выбрать опцию «Отключен» (см. рисунок 2.37);

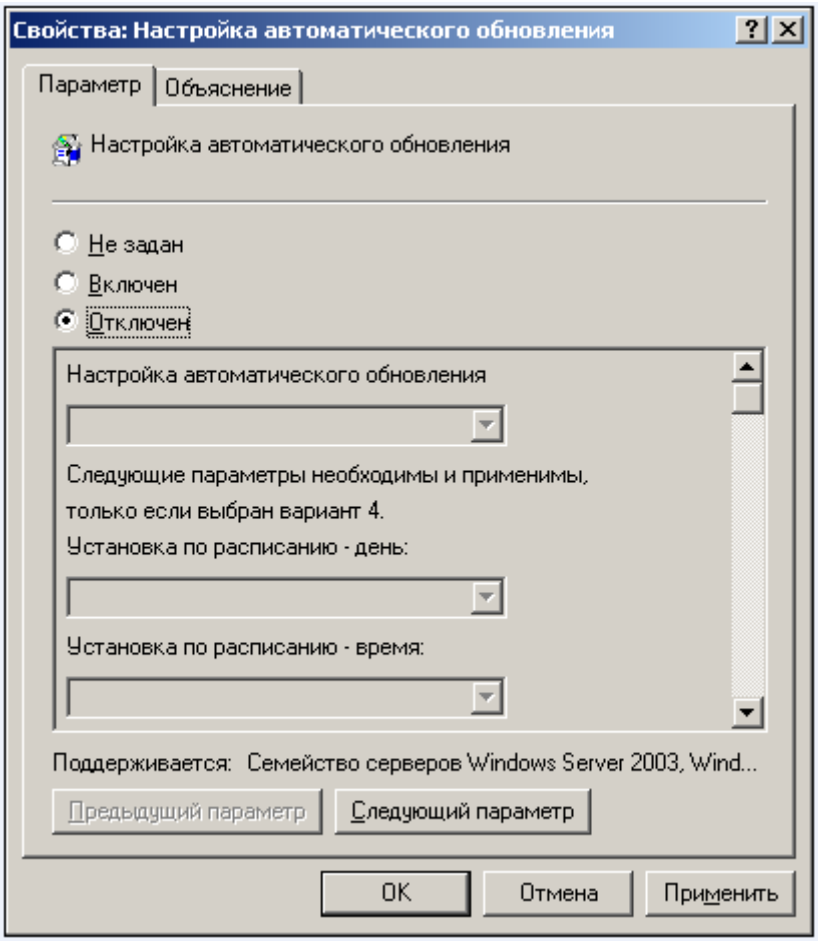


Рисунок 2.37

– закрыть редактор объекта групповой политики;
– посредством команды gpupdate.exe /force осуществить обновление параметров безопасности локальной политики безопасности.

Для отключения компонента системы «Автоматическое обновление» с помощью групповой политики, определяемой в домене Active Directory, необходимо выполнить следующие действия:

– на контроллере домена осуществить вход в систему с использованием учетной записи администратора домена;
– нажать кнопку «Пуск» и выбрать пункт «Выполнить…»;
– в поле «Открыть» диалогового окна «Запуск программы» набрать команду dsa.msc и нажать «ОК»;

- выбрать правой кнопкой мыши организационное подразделение или домен, для которого необходимо определить политику безопасности, и в контекстном меню выбрать пункт «Свойства»;
- открыть вкладку «Групповая политика», выбрать соответствующий объект групповой политики и нажать кнопку «Изменить» (в случае создания нового объекта групповой политики необходимо выбрать «Создать», ввести имя нового объекта групповой политики и нажать «Изменить»);
- в окне редактора групповой политики выбрать узел «Конфигурация компьютера» и перейти к разделу «Административные шаблоны»;
- правой кнопкой мыши нажать на элемент «Административные шаблоны» и в появившемся окне контекстного меню выбрать команду «Добавление и удаление шаблонов»;
- нажать «Добавить», в открывшемся диалоговом окне выбора шаблонов политик выбрать файл административного шаблона `Wuau.adm`, расположенный в папке `%SystemRoot%\Inf`, и нажать кнопку «Открыть»;
- выбрать параметр политики «`Настройка автоматического обновления`» и посредством двойного нажатия открыть диалоговое окно его свойств;
- на вкладке «Параметр» выбрать опцию «`Отключен`»;
- закрыть редактор объекта групповой политики;
- посредством команды `gpupdate.exe /force` осуществить обновление параметров групповой политики.

2.8 Порядок отключения возможности самостоятельной смены пароля пользователем

Установленные значения параметров безопасности политики паролей не исключают возможности самостоятельной смены пользователями значения пароля значительно раньше истечения максимального срока его действия.

С целью предотвращения смены пароля пользователем по собственному желанию до истечения срока его действия и изменения пароля только по запросу системы, администратором безопасности для компьютеров под управлением операционной системы Microsoft® Windows Servertм 2003 в различных конфигурациях безопасности с использованием административных шаблонов (файл с расширением `*.adm`, содержащий все сведения о политике на основе реестра, применяемые для настройки компьютера или среды

пользователя) может быть определена соответствующая политика. Использование данной политики позволит отключить меню «Смена пароля» в диалоговом окне «Безопасность Windows», которое появляется при нажатии пользователем сочетания клавиш Ctrl+Alt+Del, обеспечив в тоже время смену пароля пользователем по запросу системы.

Настройку политики предотвращения смены пароля пользователем по собственному желанию необходимо осуществлять с использованием редактора соответствующего объекта групповой политики в следующем разделе пространства имен объекта групповой политики: Конфигурация пользователя\Административные шаблоны\Система\Возможности CTRL+ALT+DEL.

В случае, если операционная система Microsoft® Windows Servertм 2003 функционирует на автономном компьютере, который не входит в состав домена Active Directory параметры безопасности должны определяться для каждого компьютера вручную через локальную политику безопасности. В случае, если операционная система Microsoft® Windows Servertм 2003 функционирует на компьютере, входящем в состав домена Active Directory, настройку параметров безопасности необходимо осуществлять через использование групповых политик, применяемых на уровне домена или организационных подразделений (контейнеров, содержащих учетные записи пользователей), что позволит автоматически применить требуемую конфигурацию безопасности для всех пользователей, на которые распространяется групповая политика.

Для реализации политики предотвращения смены пароля пользователями необходимо выполнить следующие действия:

1. Вызвать редактор объектов групповой политики. Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Выполнить…», в поле «Открыть» диалогового окна «Запуск программы» набрать команду mmc и нажать «ОК».

2. В открывшемся окне консоли управления ММС через пункт меню «Добавить или удалить оснастку» добавить оснастку «Редактор объектов групповой политики» и по запросу выбрать соответствующий объект групповой политики, применяемый на требуемом уровне иерархии объектов Active Directory (изменяемая групповая политика должна применяться к учетным записям пользователей, а не компьютеров).

3. В окне редактора объектов групповой политики выбрать узел «Конфигурация пользователя» и перейти к разделу «Административные шаблоны».

4. Выделить папку «Система», далее «Возможности CTRL+ALT+DEL» и перейти в левую часть окна редактора объектов групповой политики.

5. Посредством двойного нажатия параметра безопасности «Запретить изменение пароля» вызвать диалоговое окно и назначить рекомендованное для данного параметра значение (см. рисунок 2.38).

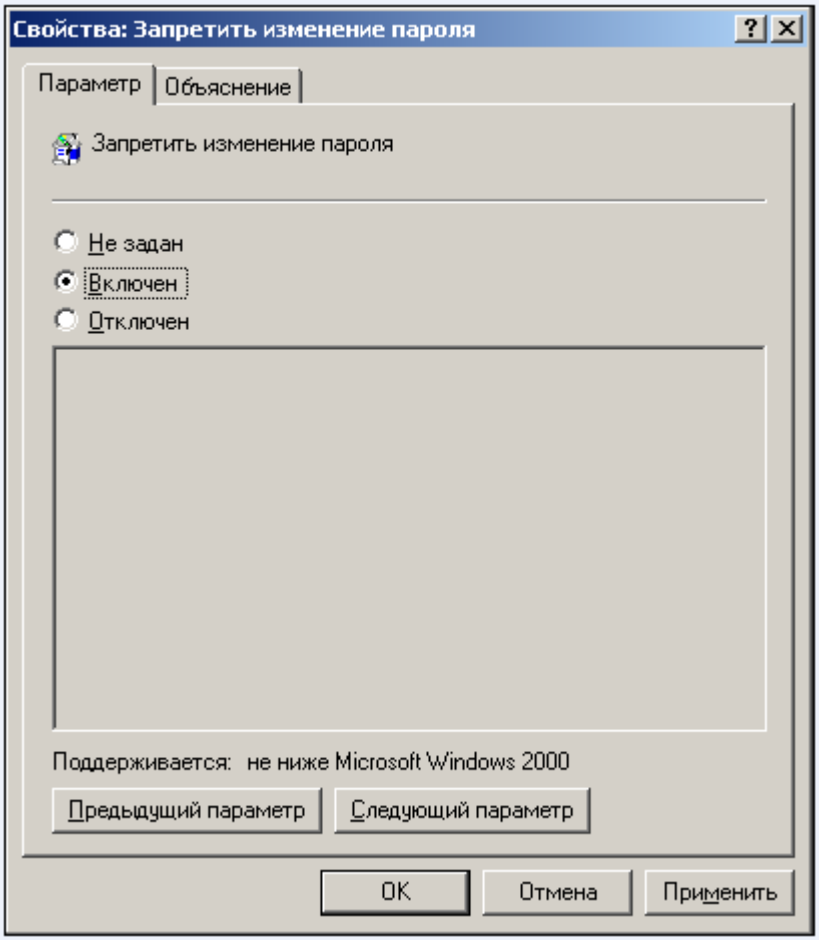


Рисунок 2.38

6. Закрыть редактор объектов групповой политики.

7. Посредством команды `gpupdate /target:user /force` осуществить обновление пользовательских параметров групповой политики.

2.9 Настройка дополнительных параметров безопасности операционной системы Microsoft® Windows Server™ 2003 с использованием реестра

Настройка дополнительных параметров безопасности операционной системы Microsoft® Windows Server™ 2003 с использование реестра позволит обеспечить большую защищенность ОС от различных типов угроз.

В данном подразделе представлено детальное описание и рекомендуемые значения ключей реестра, определяющих наиболее важные параметры безопасности серверов под управлением сертифицированной ОС Microsoft® Windows Server™ 2003 Данные параметры безопасности включены в применяемые к системе шаблоны безопасности, однако их просмотр и редактирование с использованием оснастки консоли управления «Редактор объекта групповой политики» или «Шаблоны безопасности» без выполнения дополнительных действий невозможно.

Для обеспечения возможности просмотра и дальнейшего редактирования дополнительных параметров безопасности с использованием графического интерфейса редактора конфигурации безопасности Security Configuration Editor (редактор SCE используется оснастками «Шаблоны безопасности», «Анализ и настройка безопасности», а также оснасткой «Редактор объектов групповой политики» в части настройки параметров безопасности в разделе пространства имен объекта групповой политики `Локальные политики\Параметры безопасности`), соответствующие значения ключей реестра необходимо добавить в файл `Sceregvl.inf`, расположенный в папке `%systemroot%\inf`, и перерегистрировать динамически подключаемую библиотеку редактора SCE `scecli.dll`. В результате указанных действий, дополнительные параметры безопасности будут отображаться в разделе пространства имен объекта групповой политики «`Локальные политики\Параметры безопасности`» в окне любой оснастки консоли управления Microsoft, использующей редактор SCE.

При этом изменение содержимого файла `Sceregvl.inf` и перерегистрация DLL-библиотеки `scecli.dll` может осуществляться не на каждом клиентском компьютере, на котором необходимо обеспечить настройку дополнительных параметров безопасности через реестр. Выполнив выше описанные действия на одном компьютере, администратор безопасности может создать новый шаблон безопасности, включающий расширенные настройки безопасности. Данный шаблон безопасности может быть импортирован в объект групповой политики, применяемой к одному или нескольким целевым компьютерам, независимо от того, содержат они измененный файл `Sceregvl.inf`, учитывающий дополнительные настройки безопасности, или нет.

2.9.1 Порядок настройки дополнительных параметров безопасности ОС Microsoft® Windows Servertм 2003

Для обеспечения самостоятельной настройки дополнительных параметров безопасности операционной системы Microsoft® Windows Server™ 2003 администратором безопасности необходимо выполнить следующие действия:

1. Открыть с использованием текстового редактора (например, «Блокнот») файл `%systemroot%\inf\sceregvl.inf`.

2. Перейти в раздел `[Register Registry Values]` и вставить следующий текст (каждая политика должна быть представлена одной строкой, не содержащей разрывов):

```
;============================== MSS Values ==============================
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        EnableICMPRedirect,4,%EnableICMPRedirect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        SynAttackProtect,4,%SynAttackProtect%,3,
        0|%SynAttackProtect0%,
        1|%SynAttackProtect1%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        EnableDeadGWDetect,4,%EnableDeadGWDetect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        EnablePMTUDiscovery,4,%EnablePMTUDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        KeepAliveTime,4,%KeepAliveTime%,3,
        150000|%KeepAliveTime0%,
        300000|%KeepAliveTime1%,
        600000|%KeepAliveTime2%,
        1200000|%KeepAliveTime3%,
        2400000|%KeepAliveTime4%,
        3600000|%KeepAliveTime5%,
        7200000|%KeepAliveTime6%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        DisableIPSourceRouting,4,%DisableIPSourceRouting%,3,
        0|%DisableIPSourceRouting0%,
        1|%DisableIPSourceRouting1%,
        2|%DisableIPSourceRouting2%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        TcpMaxConnectResponseRetransmissions,4,
        %TcpMaxConnectResponseRetransmissions%,
        3,0|%TcpMaxConnectResponseRetransmissions0%,
        1|%TcpMaxConnectResponseRetransmissions1%,
        2|%TcpMaxConnectResponseRetransmissions2%,
```

```
        3|%TcpMaxConnectResponseRetransmissions3%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        TcpMaxDataRetransmissions,4,%TcpMaxDataRetransmissions%,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        PerformRouterDiscovery,4,%PerformRouterDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\
        TCPMaxPortsExhausted,4,%TCPMaxPortsExhausted%,1
MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\
        NoNameReleaseOnDemand,4,%NoNameReleaseOnDemand%,0
MACHINE\System\CurrentControlSet\Control\FileSystem\
        NtfsDisable8dot3NameCreation,4,
        %NtfsDisable8dot3NameCreation%,0
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
        Explorer\NoDriveTypeAutoRun,4,%NoDriveTypeAutoRun%,3,
        0|%NoDriveTypeAutoRun0%,
        255|%NoDriveTypeAutoRun1%
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\
        WarningLevel,4,%WarningLevel%,3,
        50|%WarningLevel0%,
        60|%WarningLevel1%,
        70|%WarningLevel2%,
        80|%WarningLevel3%,
        90|%WarningLevel4%
MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\
        ScreenSaverGracePeriod,4,%ScreenSaverGracePeriod%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\
        DynamicBacklogGrowthDelta, 4,%DynamicBacklogGrowthDelta%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\
        EnableDynamicBacklog,4,%EnableDynamicBacklog%,0
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\
        MinimumDynamicBacklog,4,%MinimumDynamicBacklog%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\
        MaximumDynamicBacklog,4,%MaximumDynamicBacklog%,3,
        10000|%MaximumDynamicBacklog0%,
        15000|%MaximumDynamicBacklog1%,
        20000|%MaximumDynamicBacklog2%,
        40000|%MaximumDynamicBacklog3%,
        80000|%MaximumDynamicBacklog4%,
        160000|%MaximumDynamicBacklog5%
MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\
        SafeDllSearchMode,4,%SafeDllSearchMode%,0
```

```
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlog\
        AutoAdminLogon,4,%DisableAutoLogon%,0
MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\
        AutoShareWks,4,%AdminShares%,0
MACHINE\System\CurrentControlSet\Services\IPSEC\
        NoDefaultExempt,4,%IPSecNoDefaultExempt%,0
MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\
        Hidden,4,%HideFromBrowseList%,0
```

3. Перейти к разделу `[Strings]` и вставить следующий текст (название каждого из перечисляемых параметров должно быть представлено одной строкой, не содержащей разрывов; каждое из возможных значений параметра также должно быть представлено отдельной строкой):

```
;============================ MSS Settings ==============================
EnableICMPRedirect = "MSS: (EnableICMPRedirect) Allow ICMP redirects to
      override OSPF generated routes"
SynAttackProtect = "MSS: (SynAttackProtect) Syn attack protection level
      (protects against DoS)"
      SynAttackProtect0 = "No additional protection, use default settings"
      SynAttackProtect1 = "Connections time out sooner if a SYN attack is
      detected"
EnableDeadGWDetect = "MSS: (EnableDeadGWDetect) Allow automatic detection
      of dead network gateways (could lead to DoS)"
EnablePMTUDiscovery = "MSS: (EnablePMTUDiscovery ) Allow automatic
      detection of MTU size (possible DoS by an attacker using a small
      MTU)"
KeepAliveTime = "MSS: How often keep-alive packets are sent in
      milliseconds"
      KeepAliveTime0 ="150000 or 2.5 minutes"
      KeepAliveTime1 ="300000 or 5 minutes (recommended)"
      KeepAliveTime2 ="600000 or 10 minutes"
      KeepAliveTime3 ="1200000 or 20 minutes"
      KeepAliveTime4 ="2400000 or 40 minutes"
      KeepAliveTime5 ="3600000 or 1 hour"
      KeepAliveTime6 ="7200000 or 2 hours (default value)"
DisableIPSourceRouting = "MSS: (DisableIPSourceRouting) IP source routing
      protection level (protects against packet spoofing)"
      DisableIPSourceRouting0 = "No additional protection, source
      routed packets are allowed"
```

DisableIPSourceRouting1 = "Medium, source routed packets ignored when IP forwarding is enabled"

DisableIPSourceRouting2 = "Highest protection, source routing is completely disabled"

TcpMaxConnectResponseRetransmissions = "MSS: (TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged"

TcpMaxConnectResponseRetransmissions0 = "No retransmission, half-open connections dropped after 3 seconds"

TcpMaxConnectResponseRetransmissions1 = "3 seconds, half-open connections dropped after 9 seconds"

TcpMaxConnectResponseRetransmissions2 = "3 & 6 seconds, half-open connections dropped after 21 seconds"

TcpMaxConnectResponseRetransmissions3 = "3, 6, & 9 seconds, half-open connections dropped after 45 seconds"

TcpMaxDataRetransmissions = "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted"

PerformRouterDiscovery = "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)"

TCPMaxPortsExhausted = "MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection"

NoNameReleaseOnDemand = "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers"

NtfsDisable8dot3NameCreation = "MSS: Enable the computer to stop generating 8.3 style filenames"

NoDriveTypeAutoRun = "MSS: Disable Autorun for all drives"

NoDriveTypeAutoRun0 = "Null, allow Autorun"

NoDriveTypeAutoRun1 = "255, disable Autorun for all drives"

WarningLevel = "MSS: Percentage threshold for the security event log at which the system will generate a warning"

WarningLevel0 = "50%"

WarningLevel1 = "60%"

WarningLevel2 = "70%"

WarningLevel3 = "80%"

WarningLevel4 = "90%"

ScreenSaverGracePeriod = "MSS: The time in seconds before the screen saver grace period expires"

DynamicBacklogGrowthDelta = "MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications"

EnableDynamicBacklog = "MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications"

```
MinimumDynamicBacklog = "MSS: (AFD MinimumDynamicBacklog) Minimum number
      of free connections for Winsock applications"
MaximumDynamicBacklog = "MSS: (AFD MaximumDynamicBacklog) Maximum number
      of 'quasi-free' connections for Winsock applications"
      MaximumDynamicBacklog0 = "10000"
      MaximumDynamicBacklog1 = "15000"
      MaximumDynamicBacklog2 = "20000"
      MaximumDynamicBacklog3 = "40000"
      MaximumDynamicBacklog4 = "80000"
      MaximumDynamicBacklog5 = "160000"
SafeDllSearchMode = "MSS: Enable Safe DLL search mode"
DisableAutoLogon = "MSS: (AutoAdminLogon) Enable Automatic Logon"
AdminShares = "MSS: (AutoShareWks) Enable Administrative Shares"
IPSecNoDefaultExempt = "MSS: (NoDefaultExempt) Enable NoDefaultExempt for
      IPSec Filtering"
HideFromBrowseList = "MSS: (Hidden) Hide Computer From the Browse List"
```

4. Сохранить сделанные в файле изменения и закрыть текстовый редактор.

5. Перерегистрировать DLL-библиотеку «scecli.dll» редактора конфигураций безопасности SCE. Для этого в командной строке ввести команду «*regsvr32 scecli.dll*». При успешном выполнении команды на экран должно быть выдано следующее диалоговое окно (см. рисунок 2.39):

Рисунок 2.39

6. Открыть редактор объектов групповой политики (порядок вызова редактора и выбора ОГП детально описан в пп.2.3 настоящего Руководства).

7. В окне редактора объектов групповой политики выбрать узел «Конфигурация компьютера» и перейти к разделу «Конфигурация Windows».

8. Выделить папку «Параметры безопасности».

9. Осуществить настройку дополнительных параметров безопасности в соответствии с рекомендациями, представленными ниже.

Настройка дополнительных параметров безопасности операционной системы Microsoft® Windows Server™ 2003 R2 SP2 может осуществляться администратором безопасности следующими способами:

– с использованием редактора реестра «regedt32.exe» путем самостоятельного создания соответствующих параметров реестра и присвоения им рекомендуемых значений;
– с использованием графического интерфейса редактора конфигурации безопасности SCE.

2.9.2 Рекомендованные значения дополнительно настраиваемых параметров безопасности ОС Microsoft® Windows Serverтм 2003

Перечень дополнительно настраиваемых параметров безопасности ОС Microsoft® Windows Server™ 2003 и соответствующие им рекомендуемые для каждой конфигурации значения представлены в таблице 2.5.

Таблица 2.5

№ п/п	Название параметра	Принимаемое параметром значение
1.	MSS: Разрешить переадресацию ICMP для отмены генерируемых OSPF маршрутов. (MSS: Allow ICMP redirects to override OSPF generated routes)	Отключен
2.	MSS: Уровень защиты от SYN-атак. (MSS: SYN-attack protection level)	Connections time -out more quickly if a SYN attack is detected
3.	MSS: Разрешить автоматическое обнаружение недоступных (нефункционирующих) шлюзов. (MSS: Allow automatic detection of dead network gateways)	Отключен
4.	MSS: Разрешить автоматическое определение максимального размера пакета данных (MTU). (MSS: Allow automatic detection of MTU size)	Отключен
5.	MSS: Частота (в миллисекундах) посылки пакетов проверки доступности соединения. (MSS: How often keep-alive packets are sent in milliseconds)	300000

№ п/п	Название параметра	Принимаемое параметром значение
6.	MSS: Уровень защиты маршрутизации сообщений от источника IP. (MSS: IP source routing protection level)	Highest protection, source rou-ting is completely disabled
7.	MSS: Продолжительность рет-рансляции SYN-ACK-пакетов в случае неполучения подтверждения на запрос установления соединения. (MSS: SYN-ACK retransmissions when a connection request is not acknowledged)	3 seconds, half-open connections dropped after 9 seconds
8.	MSS: Количество попыток ретрансляции неподтвержденных данных. (MSS: How many times unacknowledged data is retransmitted)	3
9.	MSS: Разрешить использование IRDP для автоматического обнаружения и конфигурирования шлюза по умолчанию. (MSS: Allow IRDP to detect and configure Default Gateway ad-dresses)	Отключен
10.	MSS: Количество отклоненных запросов на установление соединений для инициализации защиты от SYN-атак. (MSS: How many dropped connect requests to initiate SYN attack protection)	5
11.	MSS: Запрет автоматической генерации системой имен файлов в формате 8.3 (MSS: Enable the computer to stop generating 8.3 style filenames)	Включен
12.	MSS: Запретить функцию автозапуска для всех устройств (MSS: Disable Autorun for all drives)	255, disable Autorun for all drives
13.	MSS: Время задержки между запуском режима заставки и блокировкой пользовательского сеанса (MSS: The time in seconds before the screen saver grace period ex-pires)	0

№ п/п	Название параметра	Принимаемое параметром значение
14.	MSS: Пороговое значение (в процентах) выдачи предупреждения при заполнении журнала безопасности (MSS: Percentage threshold for the security event log at which the system will generate a warning)	90%
15.	MSS: Разрешить режим безопасного поиска DLL (MSS: Enable Safe DLL search mode)	Включен
16.	MSS: Разрешить компьютеру игнорировать все запросы на разрешения имен NetBIOS за исключением WINS-серверов. (MSS: Allow the computer to ignore NetBIOS name release requests except from WINS servers)	Включен

Параметр «`MSS: Разрешить переадресацию ICMP для отмены генерируемых OSPF маршрутов`» определяет возможность переадресации системой ICMP-сообщений, что приводит к образованию некорректных маршрутов, отменяющих маршруты, полученные с использованием протокола маршрутизации OSPF (Open Shortest Path Fist), и тем самым к неверной маршрутизации всего сетевого трафика в вычислительной сети. Таким образом, возможность переадресации ICMP-сообщений для отмены генерируемых OSPF маршрутов должна быть отключена.

При настройке дополнительных параметров безопасности с использованием редактора реестра для отключения возможности переадресации ICMP для отмены генерируемых OSPF маршрутов необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
       Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
   Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  EnableICMPRedirect
  Тип данных:  REG_DWORD
    Значение:  0
```

Параметр «`MSS: Уровень защиты от SYN-атак`» позволяет уменьшить скорость ретрансляции ответов SYN-ACK на получаемые системой запросы на синхронизацию последовательных номеров, используемых во время открытия соединения (SYN-пакетов). Таким образом, в случае реализации атак типа «отказ в обслуживании» (например, атаки

«наводнение SYN-пакетами» - SYN-flood) время тайм-аута, в течение которого система будет ожидать установление соединения будет уменьшено. В связи с этим, во всех конфигурациях безопасности функция защиты системы от SYN-атак должна быть включена.

При настройке дополнительных параметров безопасности с использованием редактора реестра для включения защиты от SYN-атак необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
       Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
  Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  SynAttackProtect
  Тип данных:  REG_DWORD
    Значение:  1
```

Параметр «MSS: Разрешить автоматическое обнаружение недоступных (нефункционирующих) шлюзов» определяет возможность использования системой функции обнаружения недоступных (нефункционирующих) шлюзов, позволяющей ей автоматически переключаться на альтернативный шлюз при невозможности использования первичного шлюза.

При отсутствии запрета на использование системой функции автоматического обнаружения недоступных (нефункционирующих) шлюзов, злоумышленник может вынудить сервер переключиться на ложный шлюз. В связи с этим, во всех конфигурациях безопасности функция обнаружения недоступных (нефункционирующих) шлюзов должна быть запрещена.

При настройке дополнительных параметров безопасности с использованием редактора реестра для отключения функции обнаружения недоступных (нефункционирующих) шлюзов необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
       Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
  Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  EnableDeadGWDetect
  Тип данных:  REG_DWORD
    Значение:  1
```

Параметр «MSS: Разрешить автоматическое определение максимального размера пакета данных (MTU)» определяет возможность системы автоматически определять либо максимальную возможную единицу передачи данных MTU (Maximum Transmission Unit), либо максимальный размер пакета данных, который можно передать через заданный маршрут удаленному хосту.

Если данная возможность системы разрешена, злоумышленник может организовать атаку типа «отказ в обслуживании», основанную на использовании очень маленького значения MTU, вызвав максимальное использование компьютером всех имеющихся вычислительных ресурсов для фрагментации большого числа пакета данных. Поскольку фрагментация оказывает отрицательное влияние на функционирования системы при обработке сетевого трафика, во всех конфигурациях безопасности данная функция должна быть отключена (что приводит к установлению размера MTU равным 576 байт).

При настройке дополнительных параметров безопасности с использованием редактора реестра для отключения функции автоматическое определение максимального размера пакета данных (MTU) необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
       Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
   Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  EnablePMTUDiscovery
  Тип данных:  REG_DWORD
    Значение:  1
```

Параметр «MSS: Частота (в миллисекундах) посылки пакетов проверки доступности соединения» определяет, как часто система будет осуществлять проверку доступности неактивного соединения, посылая специальный пакет (keep-alive) данных. В случае доступности удаленного хоста он подтверждает получение пакета данных, что свидетельствует о доступности соединения.

В случае если указанному параметру присвоено большое значение (значение по умолчанию составляет 2 часа), злоумышленник, имеющий подключение к вычислительной сети, может создать предпосылки к реализации атак типа «отказ в обслуживании», установив множество неактивных соединений с атакуемой системой, которая данные соединения будет поддерживать, выделяя собственные вычислительные ресурсы, что в конечном итоге приведет к их истощению. Для обеспечения возможности противостояния указанной угрозе для данного параметра рекомендуется установить значение, равное 300000 миллисекундам.

При настройке дополнительных параметров безопасности с использованием редактора реестра для задания частоты посылки пакетов проверки доступности соединения необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
       Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
   Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  KeepAliveTime
  Тип данных:  REG_DWORD
```

```
Значение:  1
```

Параметр «MSS: Уровень защиты маршрутизации сообщений от источника IP» определяет, будет ли система использовать указанную технологию для определения маршрута, которым дейтаграммы должна следовать через вычислительную сеть. При использовании маршрутизации сообщений от источника компьютеру разрешается посылать пакет данных, в заголовке которого указан маршрут, которым он должен следовать. Однако злоумышленник может использовать указанную возможность для организации сетевой атаки, основанной на спуфинге (spoofing) сетевых пакетов. В связи с этим, во всех конфигурациях безопасности функция маршрутизации источником должна быть запрещена.

При настройке дополнительных параметров безопасности с использованием редактора реестра для задания уровня защиты маршрутизации источником IP необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
     Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
  Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  DisableIPSourceRouting
  Тип данных:  REG_DWORD
   Значение:  2
```

Параметр «MSS: Продолжительность ретрансляции SYN-ACK-пакетов в случае неполучения подтверждения на запрос установления соединения» определяет временной интервал, в течение которого система будет ретранслировать SYN-ACK-пакеты, перед тем как прекратить попытки установления соединения. При этом задержка (тайм-аут) ретрансляции увеличивается вдвое при каждой последующей попытки подключения. Рекомендуемое значение тайм-аута составляет 3 секунды. Таким образом, в случае реализации атаки «наводнение SYN-пакетами» (SYN-flood) время, в течение которого система будет ожидать установление соединения, составит 9 секунд, по прошествии которых полуоткрытые соединения будут автоматически закрыты.

При настройке дополнительных параметров безопасности с использованием редактора реестра для задания продолжительности временного интервала ретрансляция SYN-ACK-пакетов необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
     Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
  Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  TcpMaxConnectResponseRetransmissions
  Тип данных:  REG_DWORD
   Значение:  2
```

Параметр «MSS: Количество попыток ретрансляции неподтвержденных данных» определяет количество попыток, которые предпринимаются системой для ретрансляции конкретного сегмента данных, перед тем как соединение будет закрыто. Рекомендуемое значение попыток ретрансляции составляет 3 раза. Таким образом, в случае реализации атаки «наводнение SYN-пакетами» (SYN-flood) система выполнит только три попытки ретрансляции неподтвержденных данных, исчерпав которые, автоматически закроет соединения.

При настройке дополнительных параметров безопасности с использованием редактора реестра для задания количества попыток ретрансляции неподтвержденных данных необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
    Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  TcpMaxDataRetransmissions
  Тип данных:  REG_DWORD
    Значение:  3
```

Параметр «MSS: Разрешить использование IRDP для автоматического обнаружения и конфигурирования шлюза по умолчанию» используется для разрешения или запрета использования системой протокола обнаружения маршрутизаторов IRDP (Internet Router Discovery Protocol), которые позволяет ей автоматически определять адрес маршрутизатора и использовать его в качестве стандартного шлюза по умолчанию.

Данная возможность может быть использована злоумышленником и заключается в компрометации одного из компьютеров, находящихся в едином сегменте вычислительной сети, и настройка его в качестве ложного шлюза. Таким образом, другие компьютеры с разрешенной поддержкой IDRP будут пытаться маршрутизировать собственный сетевой трафик через ложный шлюз.

Чтобы исключить возможность автоматического обнаружения и конфигурирования системой шлюза по умолчанию, поддержка протокола IDRP должна быть отключена. Для этого необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
    Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  PerformRouterDiscovery
  Тип данных:  REG_DWORD
    Значение:  0
```

Параметр «MSS: Количество отклоненных запросов на установление соединений для инициализации защиты от SYN-атак» определяет максимальное

количество отклоненных запросов на установление соединений, при достижении которого будет инициализирована защита от SYN-атак. Защита от SYN-атак задействуется в том случае, когда запрос на установление соединения был отвергнут системой по причине исчерпания существующего резерва очереди входящих соединений. Рекомендуемое значение данного параметра составляет 5. Таким образом, в случае реализации различных видов SYN-атак система автоматически инициирует защиту от них после 5 отклоненных запросов на установление входящего соединения.

При настройке дополнительных параметров безопасности с использованием редактора реестра для задания количества отклоненных запросов на установление соединений для инициализации защиты от SYN-атак необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
   Подраздел:  \CurrentControlSet\Services\Tcpip\Parameters\
Имя элемента:  TCPMaxPortsExhausted
  Тип данных:  REG_DWORD
    Значение:  5
```

Параметр «MSS: Запрет автоматической генерации системой имен файлов в формате 8.3» определяет возможность генерации операционной системой имен файлов в формате 8.3 (восемь символов выделяются для имени файла, три символа – для типа файла), для обеспечения обратной совместимости и поддержки 16-битных приложений.

Использование системой имен файлов в формате 8.3 позволит злоумышленнику использовать только восемь символов для поиска заданных файлов, вместо 20, которые могут использоваться для именования файлов. В свою очередь при использовании длинных имен поиск указанных файлов будет затруднен. В связи с этим, во всех конфигурациях безопасности должна быть запрещена возможность автоматической генерации системой имен файлов в формате 8.3.

При настройке дополнительных параметров безопасности с использованием редактора реестра для отключения функции автоматической генерации системой имен файлов в формате 8.3 необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
   Подраздел:  \CurrentControlSet\Control\FileSystem\
Имя элемента:  NtfsDisable8dot3NameCreation
  Тип данных:  REG_DWORD
    Значение:  1
```

Параметр «MSS: Запретить функцию автозапуска для всех устройств» определяет возможность немедленного чтения системой данных с медиа-носителя, как только оно было вставлено в устройство чтения. В результате этого осуществляется автоматический запуск программ, расположенных на данном носители информации.

С использованием данной функции связана потенциальная возможность автоматического запуска системой злонамеренного кода, содержащегося на медиа-носителе, который может быть вставлен злоумышленником, имеющим физический доступ к клиентскому компьютеру. Исходя их этого, во всех конфигурациях безопасности параметр «MSS: Запретить функцию автозапуска для всех устройств» должен иметь значение «255, disable Autorun for all drives» (Запретить автозапуск для всех устройств).

При настройке дополнительных параметров безопасности с использованием редактора реестра для отключения функции автозапуска для всех устройств необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\SOFTWARE
    Подраздел:  \Microsoft\Windows\CurrentVersion\Policies\Explorer\
Имя элемента:  NoDriveTypeAutoRun
  Тип данных:  REG_DWORD
    Значение:  0xFF
```

Параметр «MSS: Время задержки между запуском режима заставки и блокировкой пользовательского сеанса» определяет промежуток времени, который должен пройти между запуском режима заставки и непосредственной блокировкой сеанса пользователя, в случае если данная возможность используется в системе.

По умолчанию, установленное время задержки составляет 5 секунд, что обеспечивает возможность возврата пользователя в систему до непосредственной блокировки сеанса, исключая необходимость ввода им пароля и в тоже время возможность доступа злоумышленника в систему без прохождения процедур идентификации и аутентификации с использованием регистрационных данных пользователя, осуществившего вход. Для обеспечения возможности немедленной блокировки пользовательского сеанса при запуске режима заставки данный параметр во всех конфигурациях безопасности должен иметь значение «0».

При настройке дополнительных параметров безопасности с использованием редактора реестра для задания времени задержки между запуском режима заставки и блокировкой пользовательского сеанса необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\SOFTWARE
```

```
     Подраздел:  \Microsoft\Windows NT\CurrentVersion\Winlogon\
Имя элемента:  ScreenSaverGracePeriod
  Тип данных:  String
    Значение:  0
```

Параметр «MSS: Пороговое значение (в процентах) выдачи предупреждения при заполнении журнала безопасности» определяет процент заполненности журнала безопасности операционной системы, при достижении которого система выдаст предупреждение (в виде записи события аудита с идентификатором eventID 523).

В случае если журнал безопасности заполнен, и система не сконфигурирована не перезапись событий аудита по необходимости, то некоторые записи аудита могут быть потеряны. Если же система сконфигурирована на немедленное завершение работы при заполнении журнала безопасности, то это, в свою очередь, может привести к прекращению предоставления клиентским компьютером различного рода сервисов. В связи с этим, во всех конфигурациях безопасности пороговое значение выдачи предупреждения при заполнении журнала безопасности должно быть установлено равным 90%.

При настройке дополнительных параметров безопасности с использованием редактора реестра для задания порогового значения (в процентах) выдачи предупреждения при заполнении журнала безопасности необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
     Подраздел:  \CurrentControlSet\Services\Eventlog\Security\
Имя элемента:  WarningLevel
  Тип данных:  REG_DWORD
    Значение:  90
```

Параметр «MSS: Разрешить режим безопасного поиска DLL» определяет, каким из двух способов будет осуществляться поиск DDL-библиотек:

- сначала осуществлять поиск в папках, определенных через системную переменную path, далее в текущей рабочей папке;
- сначала осуществлять поиск в текущей рабочей папке, далее в папках, определенных через системную переменную path.

При использовании второго варианта существует вероятность того, что в случае запуска пользователем злонамеренного кода, им могут быть задействованы собственные версии системных DDL-библиотек, расположенных в текущей папке, что может увеличить уровень ущерба, который может быть им нанесен. Поэтому во всех конфигурациях

безопасности поиск системных DDL-библиотек сначала должен осуществляется в папках, определенных через системную переменную path, и только затем в текущей рабочей папке.

При настройке дополнительных параметров безопасности с использованием редактора реестра для задания режима безопасного поиска DLL-библиотек необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\SYSTEM
   Подраздел:  \CurrentControlSet\Control\Session Manager\
Имя элемента:  SafeDllSearchMode
  Тип данных:  REG_DWORD
    Значение:  1
```

Параметр «Разрешить компьютеру игнорировать все запросы на разрешения имен NetBIOS за исключением WINS-серверов» определяет возможность обработки системой запросов на разрешение собственного NetBIOS-имени, поступающих от клиентских компьютеров. Поскольку протокол NetBIOS не обеспечивает аутентификацию отправителя (компьютера, формирующего запрос на разрешение NetBIOS-имени), существует угроза посылки злоумышленником специально сформированного запроса, что приведет к отказу в обслуживании системы и прекращению обработки легитимных запросов на разрешение собственного имени. Таким образом, во всех рассматриваемых конфигурациях безопасности получение запросов на разрешение NetBIOS-имени должно быть разрешено только от WINS-серверов.

При настройке дополнительных параметров безопасности с использованием редактора реестра для включения возможности обработки запросов на разрешение NetBIOS-имени только от WINS-серверов необходимо осуществить создание (модификацию) значения следующего параметра реестра:

```
        Раздел:  HKEY_LOCAL_MACHINE\System
   Подраздел:  \CurrentControlSet\Services\LanmanServer\Parameters
Имя элемента:  NoNameReleaseOnDemand
  Тип данных:  REG_DWORD
    Значение:  1
```

3 Последовательность действий по контролю сертифицированной версии операционной системы Microsoft® Windows Server™ 2003

Контроль маркирования сертифицированной версии операционной системы Microsoft® Windows Server™ 2003 в совокупности с контролем исходного состояния, настроек безопасности, а так же контроль установленных сертифицированных обновлений безопасности, основанный на вычислении контрольных сумм, направлен на получение однозначного соответствия сертифицированной версии Microsoft® Windows Server™ 2003, тому ПО, которое установлено на рабочей станции.

3.1 Контроль маркирования сертифицированной версии операционной системы Microsoft® Windows Server™ 2003

Порядок проведения контроля маркирования:

1. Удостовериться, что комплект поставки сертифицированной версии «Microsoft® Windows® Server 2003» соответствует комплектам поставки установленного образца, и соответствует комплектности, приведенной в формуляре.

2. Удостовериться, что упаковка с дистрибутивом операционной системы, заклеена неповрежденной этикеткой со штриховым кодом и уникальным учётным номером дистрибутива (рисунок 3.1).

Рисунок 3.1 - Образец этикетки со штриховым кодом и уникальным номером дистрибутива

3. Удостовериться в том, что номер диска (указан на оптическом носителе дистрибутива ОС) и уникальный учетный номер дистрибутива (указан на этикетке с ШК), установленной на рабочей станции, соответствует номерам, указанным в разделе 2.8 Формуляра на сертифицированную версию Microsoft® Server 2003.

4. Удостовериться в том, что номера знаков соответствия ФСТЭК России (на формуляре/упаковке с дистрибутивом ОС на лицензионных стикерах ОС) соответствуют номерам, указанным в разделе 2 Формуляра на сертифицированную версию Microsoft® Windows® Server 2003.

3.2 Автоматизированный контроль сертифицированной версии операционной системы Microsoft® Windows Server™ 2003

3.2.1 Назначение программы контроля сертифицированной версии ПО «Check»

Для контроля сертифицированной версии операционной системы Microsoft® Windows Server™ 2003, а так же обновлений безопасности для неё, используется программа контроля сертифицированной версии ОС Microsoft® Windows® Server™ 2003 «Check», поставляемая дополнительно к пакету для сертифицированной версии ОС на компакт-диске Media Kit.

Программа «Check» предназначена для решения следующих задач:

- контроль сответсвия развернутой версии ОС сертифицированной;
- контроль установленных сертифицированных обновлений безопасности;
- проверку соответсвия настроек развернутой ОС сертифицированным;
- фиксацию и контроль целостности системных файлов Windows Server 2003;
- подготовку проекта аттестата соответствия.

Программа «Check» работает на локальных и сетевых компьютерах с выходом в Интернет, получая сведения с on-line базы сертифицированных обновлений. Предусмотрен режим работы на комьютерах без доступа в Интеренет. Доступ к базе сертифицированных обновлений осуществляется по цифровому сертификату, записанному на электронный ключ.

3.2.2 Установка и запуск на выполнение программы «Check»

Для установки программы необходимо выполнить следующую последовательность действий:

1) Начать сеанс Microsoft® Windows® Server 2003 с правами локального администратора.

2) Установить Net Framework 2.0 и выше (если он не установлен ранее). Для этого запустить файл DotNetFX/dotnetfx.exe с диска Media Kit и произвести процедуру инсталляции в директорию по-умолчанию.

3) Установить программу Windows Installer версии 3.1 и выше (если она не установлена). Для этого запустить файл DotNetFX/WindowsInstaller-KB893803-v2-x86.exe с диска MediaKit и произвести процедуру инсталляции в директорию по-умолчанию.

4) Произвести установку драйвера для электронного ключа eToken с записанным цифровым сертификатом организации. Для этого выполнить файл etlogon5_xp_x86.msi (или более новой версии драйвера) с диска MediaKit.

5) Загрузить с Центра сертифицированных обновлений ЗАО «АТТЭКС-СОФТ» по адресу http://www.altx-soft.ru/downloads.htm и произвести установку цифровых сертификатов удостоверяющих центров ЗАО «АЛТЭКС-СОФТ». Для этого произвести последовательную загрузку Сертификата № 1 и Сертификата №2 с сайта компании ЗАО «АЛТЭКС-СОФТ». Для этого необходимо щелкнуть мышью по соответствующей ссылке и появившемся окне нажать кнопку «Открыть» (см. рисунок 3.2). В появившемся окне нажать кнопку «Установить сертификат» (см. рисунок 3.3).

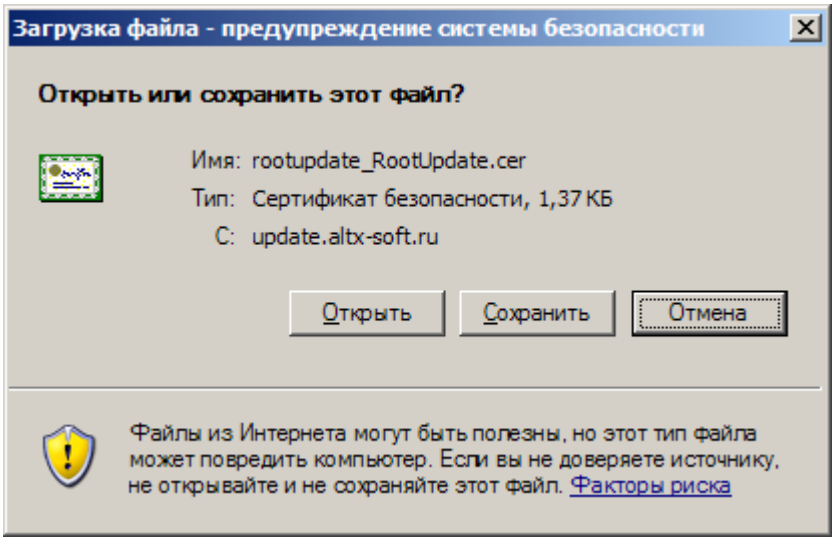


Рисунок 3.2- Открытие цифрового сертификатов удостоверяющего центра ЗАО «АЛТЭКС-СОФТ»

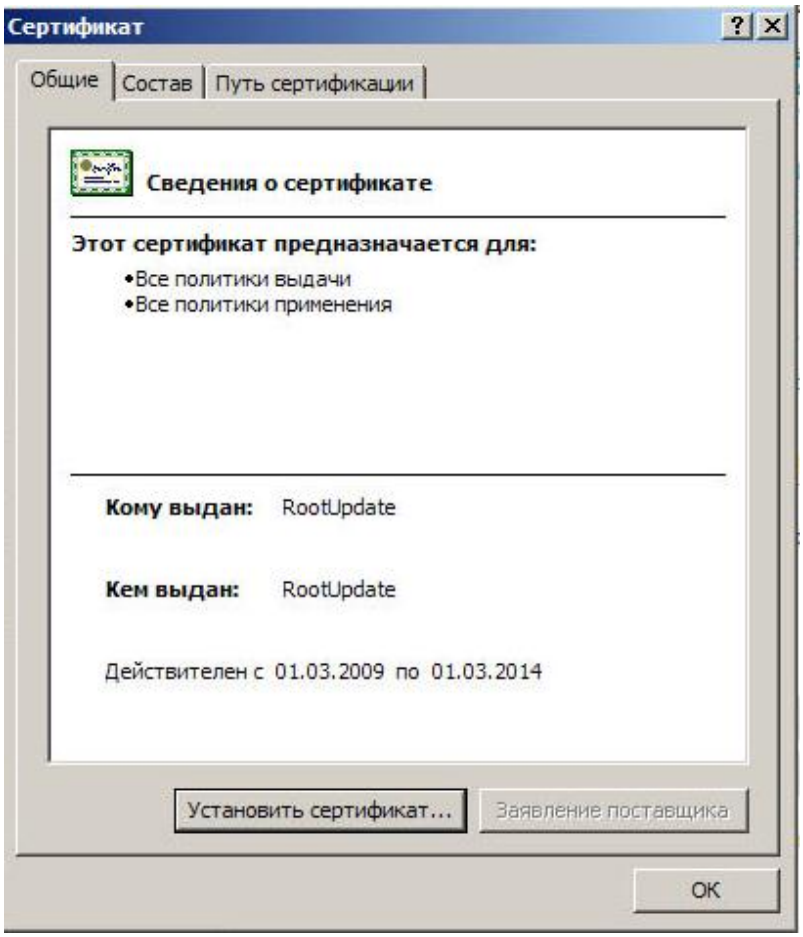


Рисунок 3.3 - Установка цифрового сертификатов удостоверяющего центра ЗАО «АЛТЭКС-СОФТ»

Примечание: а) Для обеспечения гарантированной корректной работы при наличии нескольких установленных браузеров обозревателем по-умолчанию следует устанавливать Microsoft Explorer. В противном случае для других обозревателей установленных по умолчанию может потребоваться ручная установка цифровых сертификатов (после их сохранения на локальный диск компьютера).

б) Более подробная информация о пользовании Центром сертифицированных обновлений ЗАО «АЛТЭКС-СОФТ» доступна по адресу http://www.altx-soft.ru/downloads.htm.

6) Выполнить файл setup.exe и произвести установку программы. В процессе установки программы будет предложено выбрать каталог программы и пользователей, для которых программа устанавливается.

7) Вставить электронный ключ eToken в USB-порт и произвести запуск программы «Check» выполнением файла Check.exe из каталога установки программы.

Главное окно программы представлено на рисунке 3.4.

При каждом запуске программа «Check» выполняет контроль версии контролируемой системы, в случае если версия операционной системы не соответствует сертифицированной, на экран будет выведено сообщение, представленное на рисунке 3.5.

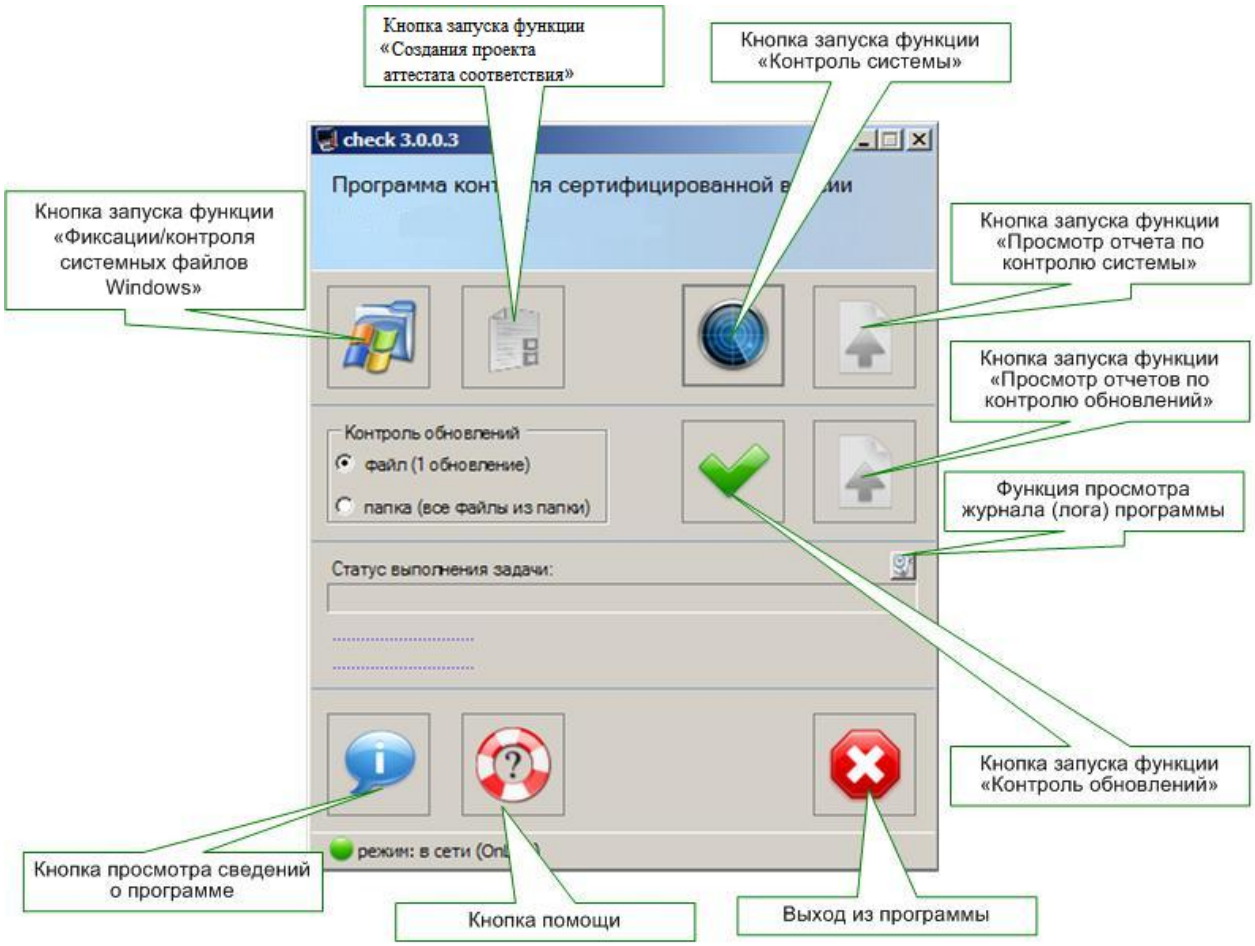


Рисунок 3.4 –Главное окно программы контроля Check

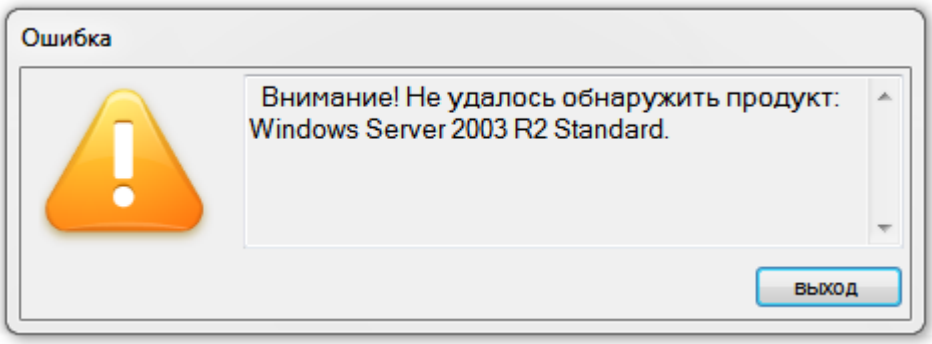


Рисунок 3.5 – Вид окна программы при несоответствии версии ОС сертифицированной

Для полнофункциональной работы программы с автоматизированного рабочего места должен присутствовать доступ в сеть Интернет, а именно к сайту по адресу; http://check.altx-soft.ru/. В случае отсутствия доступа в нижней части клиентской части программы, будет отображен индикатор 

. При этом все параметры контролируемой системы, будут сохранены в файл-отчёт offlineReport.xml. Данный отчет сохраняется в папку с установленной программой автоматически после запуска сканирования, при этом вид окна программы будет иметь вид, изображенный на рисунке 3.6.

Примечание: При отсутствии доступа к сайту следует проверить настройки брэндмауэра и антивируса и при необходимости внести выполняемый файл программы «check.exe» в число доверенных файлов.

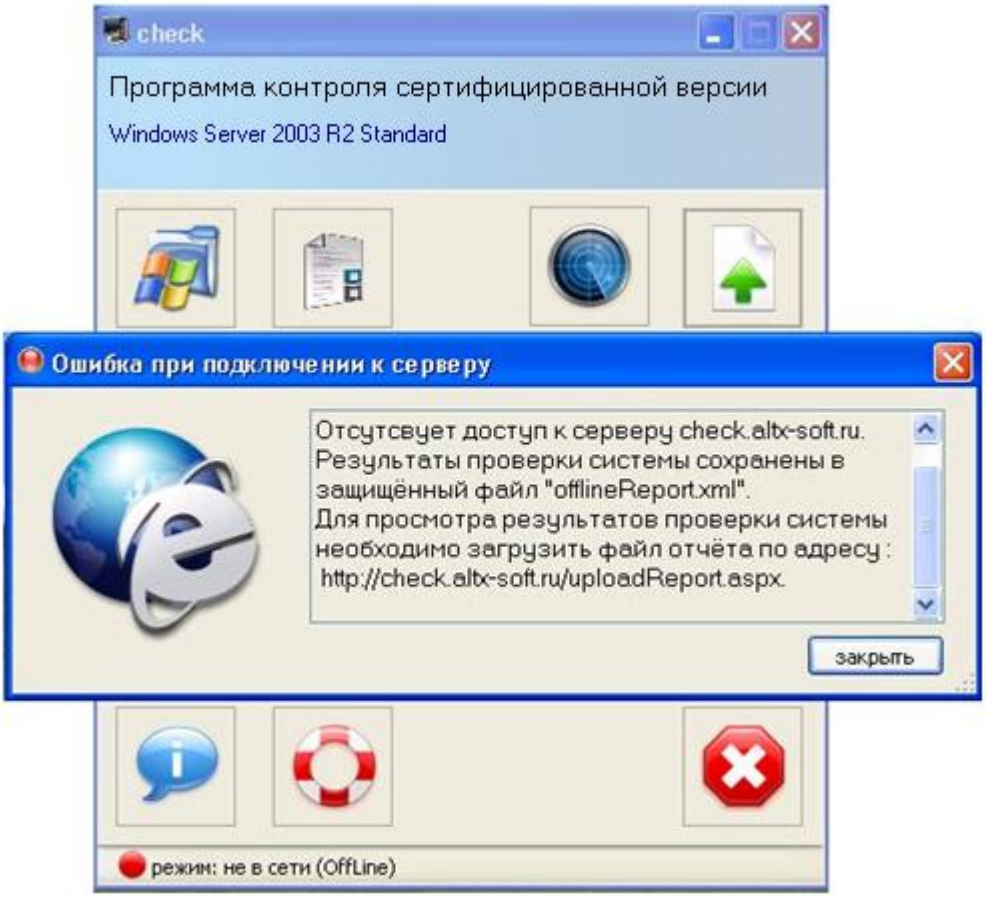


Рисунок 3.6 – Окно программы при отсутствии доступа в сеть Интернет

Сформированный при отсутствии подключения к сети Интернет файл отчета «offlineReport.xml» можно загрузить на защищенный сайт ЗАО «АЛТЭКС-СОФТ» для последующей генерации отчета (см. п.п. *Проверка сертифицированной версии Windows и просмотр отчета по контролю системы*). Для этого необходимо в окне обозревателя перейти по адресу http://check.altx-soft.ru/uploadReport.aspx и выбрать данный файл в окне выбора, представленном на рисунке 3.7.

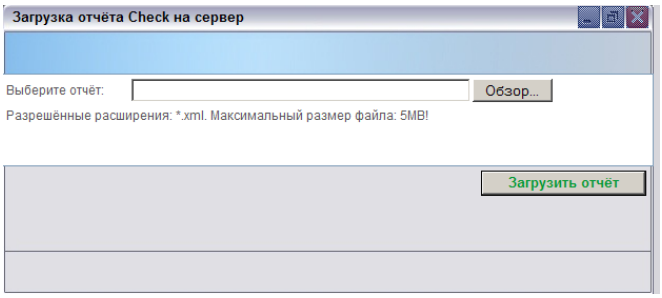


Рисунок 3.7 – Вид окна загрузки отчета программы сформированного при отсутствии подключения к сети Интернет

3.2.3 Выполнение программы «Check»

Проверка сертифицированной версии Windows Server 2003 и просмотр отчета по контролю системы

Чтобы произвести проверку соответствия установленной Microsoft Windows Server 2003 сертифицированной версии необходимо нажать кнопку 

В случае корректной установки на экран будет выведено сообщение, представленное на рисунке 3.8. После проведения проверки сертифицированной версии Windows Server 2003 становится доступной функция просмотра отчета о состоянии системы.

Просмотр отчета по контролю системы происходит при нажатии кнопки «Просмотреть отчет по контролю системы». После нажатия кнопки и ввода пароля электронного ключа e-token осуществляется переход на защищенный сайт ЗАО «АТЭКС-СОФТ», где пользователь может просмотреть результаты контроля.

В случае успешного завершение контроля, т.е. полного соответствия текущей версии операционной системы Microsoft Windows Server 2003 сертифицированной версии и установленных всех сертифицированных обновлений на экране будет отображено окно, изображенное на рисунке 3.9.

В случае соответствия текущей версии операционной системы Microsoft Windows Server 2003 сертифицированной, но отсутствии некоторых критических для безопасности системы обновлений, патчей или Service Pack на экране пользователя будет отображено окно, изображенное на рисунке 3.10, где будут указаны необходимые для установки обновлений безопасности ссылки на сайт корпорации Microsoft.

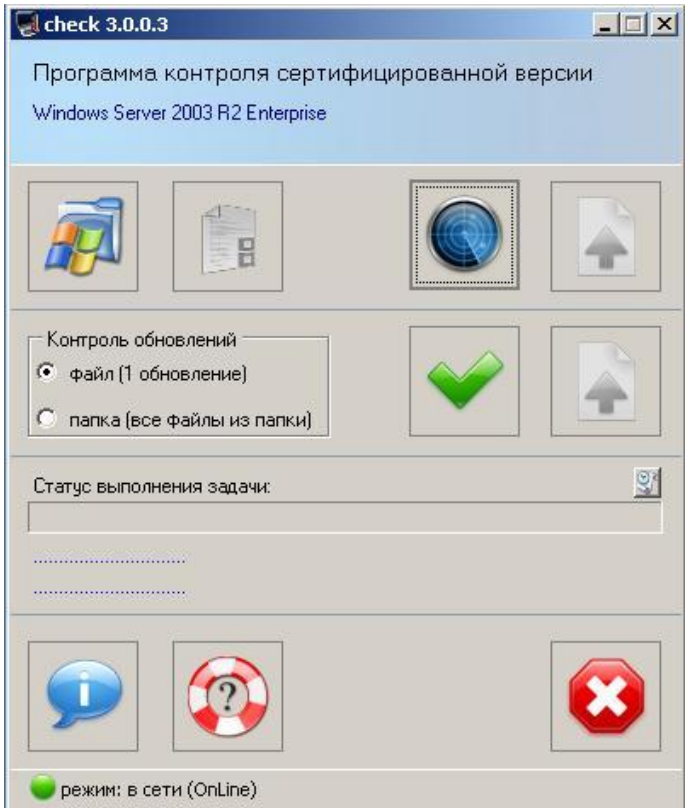


Рисунок 3.8 – Проверка сертифицированной версии Microsoft Windows Server 2003

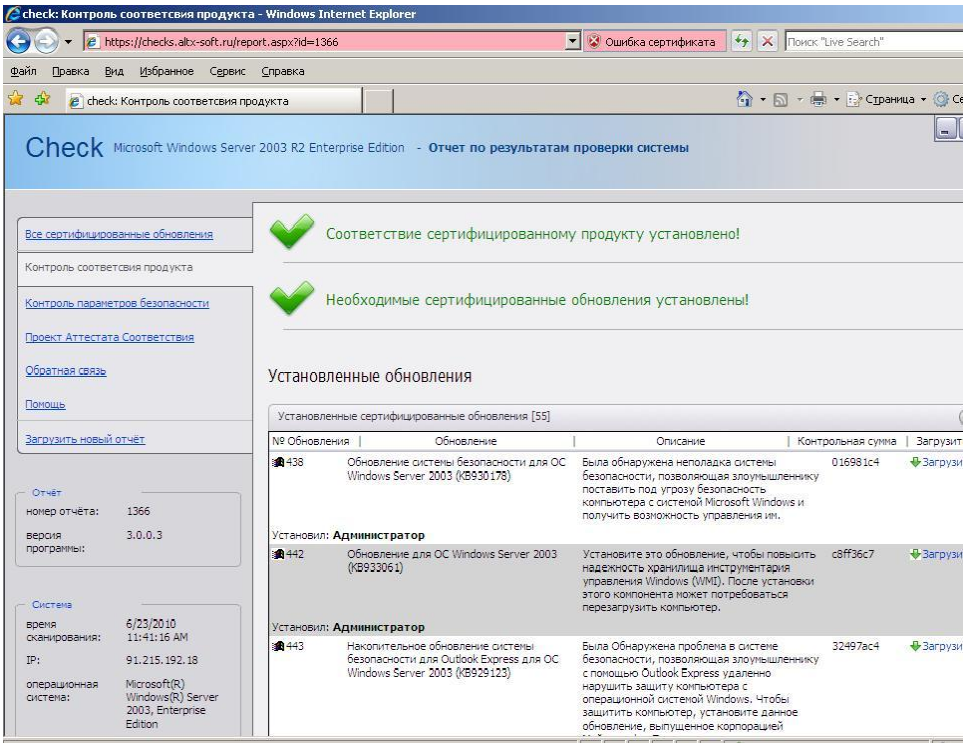


Рисунок 3.9 – Microsoft Windows Server 2003 при полном соответствии файлов и обновлений безопасности.

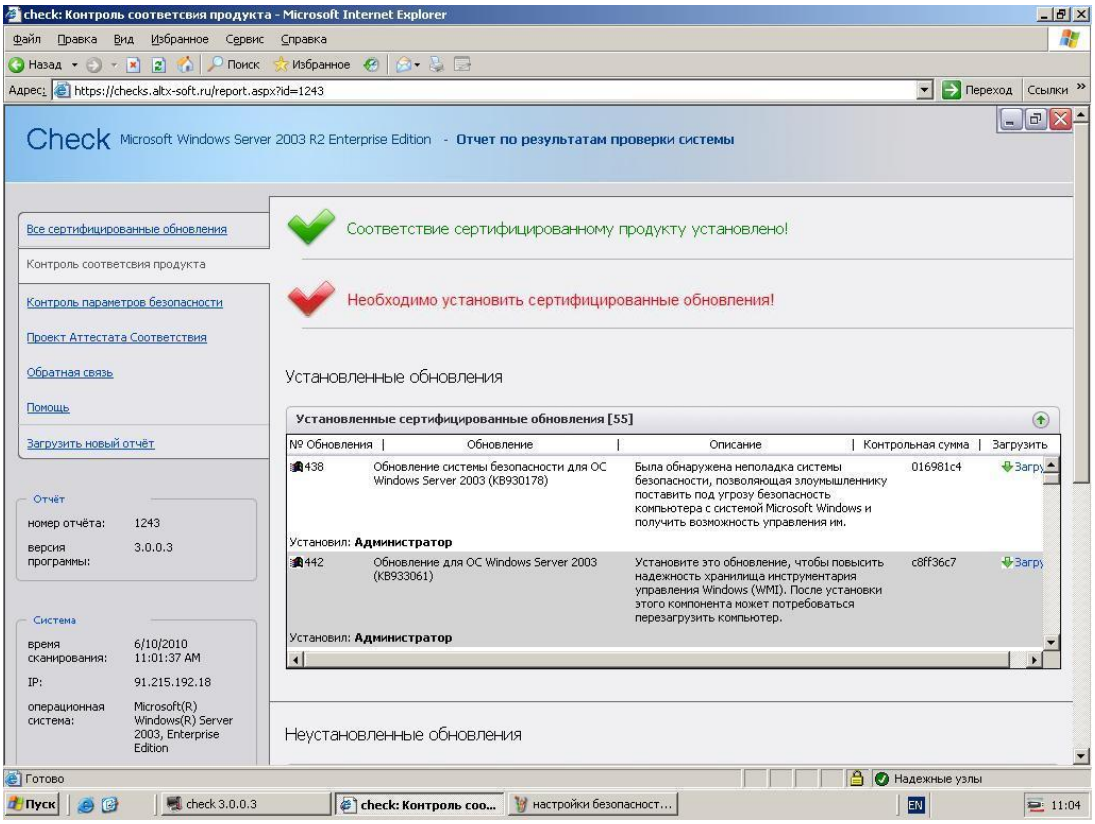


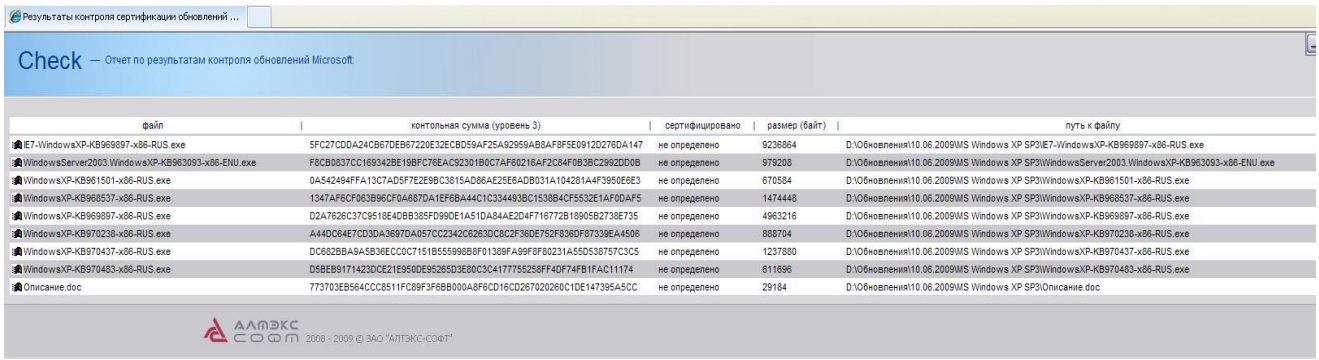
Рисунок 3.10 – Вид окна программы контроля сертифицированной версии ОС Microsoft Windows Server 2003 при неполном соответствии обновлений безопасности.

Проверка и просмотр отчета по контролю обновлений системы

Важной особенностью программы «Check», является функция автоматического контроля соответствия скачанных обновлений безопасности сертифицированным обновлениям.

Контроль обновлений можно производить для одного выбранного файла обновлений, либо для всех файлов обновлений в выбранной папке. Для запуска этой функции необходимо выбрать опцию «файл (1 обновление)», либо «папка (все файлы из папки)» переключателя «Контроль обновлений» главного окна программы, нажать кнопку главного окна программы и выбрать соответственно файл или папку с исполняемыми файлами обновлений.

После завершения проверки необходимо нажать кнопку («Просмотреть отчет по контролю обновлений»). После этого осуществляется переход на защищенный сайт ЗАО «АЛТЭКС-СОФТ», где будет произведено сравнение загруженных файлов с контрольными образами на сайте. В случае успеха на экран будет выведено окно, представленное на рисунке 3.11.



файл	контольная сумма (уровень 3)	сертифицировано	размер (байт)	путь к файлу
IE7-WindowsXP-KB969897-x86-RUS.exe	5FC27CDDA24CB67DEB67220E32ECBD59AF25A92959AB8AF8F5E0912D276DA147	не определено	9236864	D:\Обновления\10.06.2009\MS Windows XP SP3\IE7-WindowsXP-KB969897-x86-RUS.exe
WindowsServer2003.WindowsXP-KB963093-x86-ENU.exe	F8CB0837CC169342BE19BFC76EAC92301B0C7AF60216AF2C84F0B3BC2992DD0B	не определено	979208	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsServer2003.WindowsXP-KB963093-x86-ENU.exe
WindowsXP-KB961501-x86-RUS.exe	0A542494FFA13C7AD5F7E2E9BC3815AD86AE25E6ADB031A104281A4F3950E6E3	не определено	670584	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB961501-x86-RUS.exe
WindowsXP-KB968537-x86-RUS.exe	1347AF6CF063B96CF0A687DA1EF6BA44C1C334493BC1538B4CF5532E1AF0DAF5	не определено	1474448	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB968537-x86-RUS.exe
WindowsXP-KB969897-x86-RUS.exe	D2A7626C37C9518E4DBB385FD99DE1A51DA84AE2D4F716772B18905B2738E735	не определено	4963216	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB969897-x86-RUS.exe
WindowsXP-KB970238-x86-RUS.exe	A44DC64E7CD3DA3697DA057CC2342C6263DC8C2F36DE752F836DF87339EA4506	не определено	888704	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB970238-x86-RUS.exe
WindowsXP-KB970437-x86-RUS.exe	DC682BBA9A5B36ECC0C7151B555998B8F01389FA99F8F80231A55D538757C3C5	не определено	1237880	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB970437-x86-RUS.exe
WindowsXP-KB970483-x86-RUS.exe	D5BEB9171423DCE21E950DE95265D3E80C3C4177755258FF4DF74FB1FAC11174	не определено	611696	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB970483-x86-RUS.exe
Описание.doc	773703EB564CCC8511FC89F3F6BB000A8F6CD16CD267020260C1DE147395A5CC	не определено	29184	D:\Обновления\10.06.2009\MS Windows XP SP3\Описание.doc

Рисунок 3.12 – Вид окна с результатами контроля текущих обновлений ОС сертифицированным

При нажатии вкладки «Все сертифицированные обновления», пользователю будет отображен полный список установленных на контролируемой системе обновлений (см. рисунок 3.12).

В случае, если соответствие файлов ОС, установленной на ПЭВМ, и файлов сертифицированной ОС Microsoft Windows Server 2003 не установлено, в окне программы будет выведена надпись «Соответствие сертифицированной ОС не установлено» и весь функционал программы будет недоступен пользователю.

Фиксация и контроль системных файлов Microsoft Windows Server 2003

Операция фиксации и контроля системных файлов Microsoft Windows Server 2003 производится при нажатии кнопки  главного окна программы (см. рисунок 3.13).

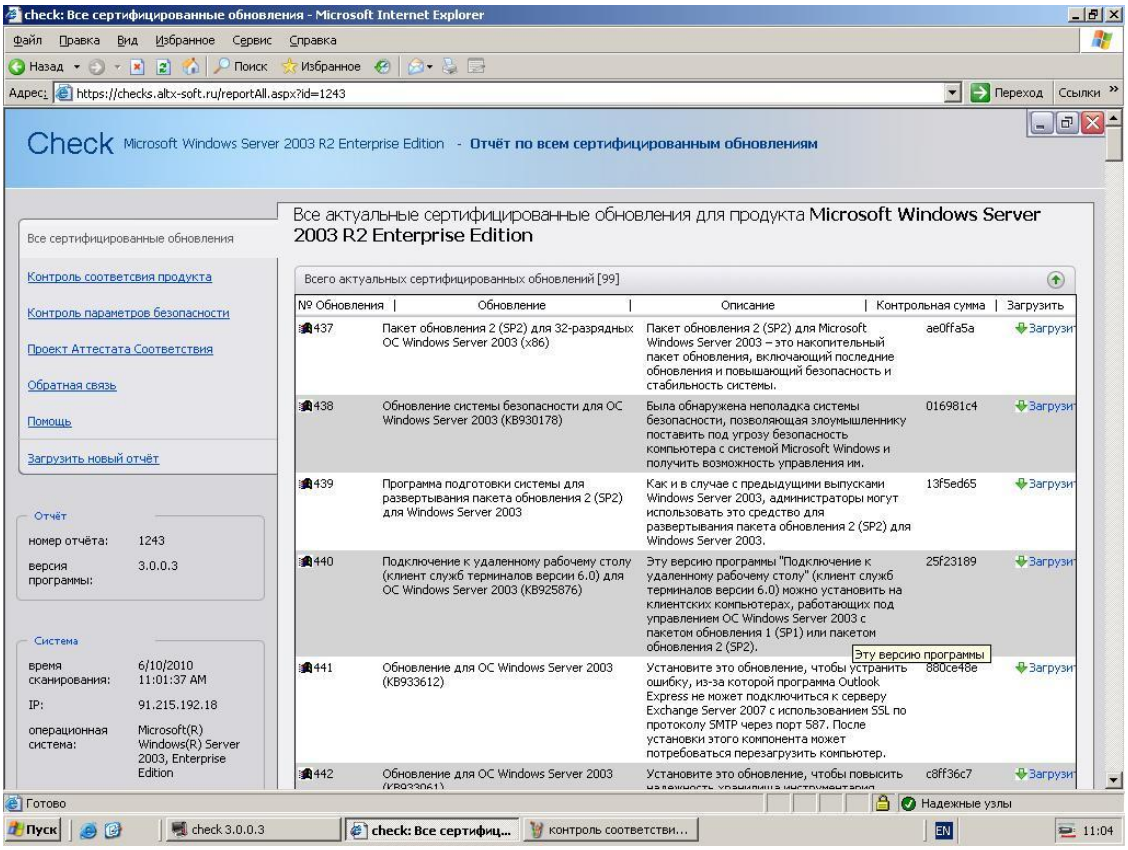


Рисунок 3.12 – Вид окна программы контроля сертифицированной версии Microsoft Windows Server 2003 после выбора вкладки «Все сертифицированные обновления»

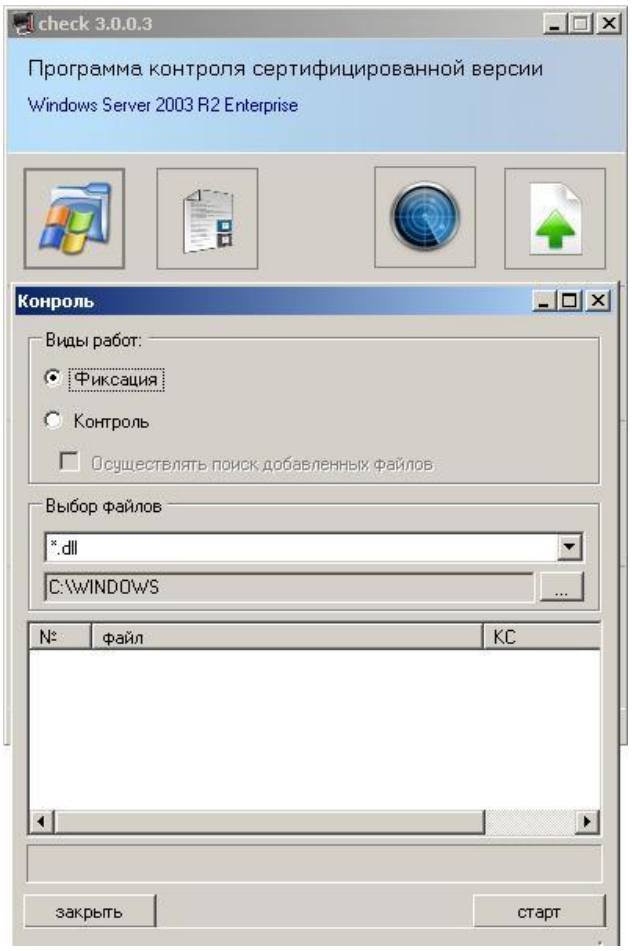


Рисунок 3.13 – Вид окна программы при проведении фиксации или контроля исходного состояния файлов ОС Microsoft Windows Server 2003

Для проведения фиксации исходного состояния необходимо установить переключатель «Вид работы» в положение «Фиксация». По умолчанию в поле «Выбор файлов» указана маска, предполагающая проведение фиксации всех файлов операционной системы. При такой установке будет произведена фиксация всех файлов находящихся в системной папке Windows, что может занять длительное время. С целью уменьшения времени фиксации могут быть указаны другие маски, задаваемые вручную, или путем выбора из списка. Вызов списка осуществляется путем нажатия кнопки , расположенной в правой части поля «Выбор файлов». После нажатия кнопки «Старт», окно программы приобретет вид, показанный на рисунке 3.14.

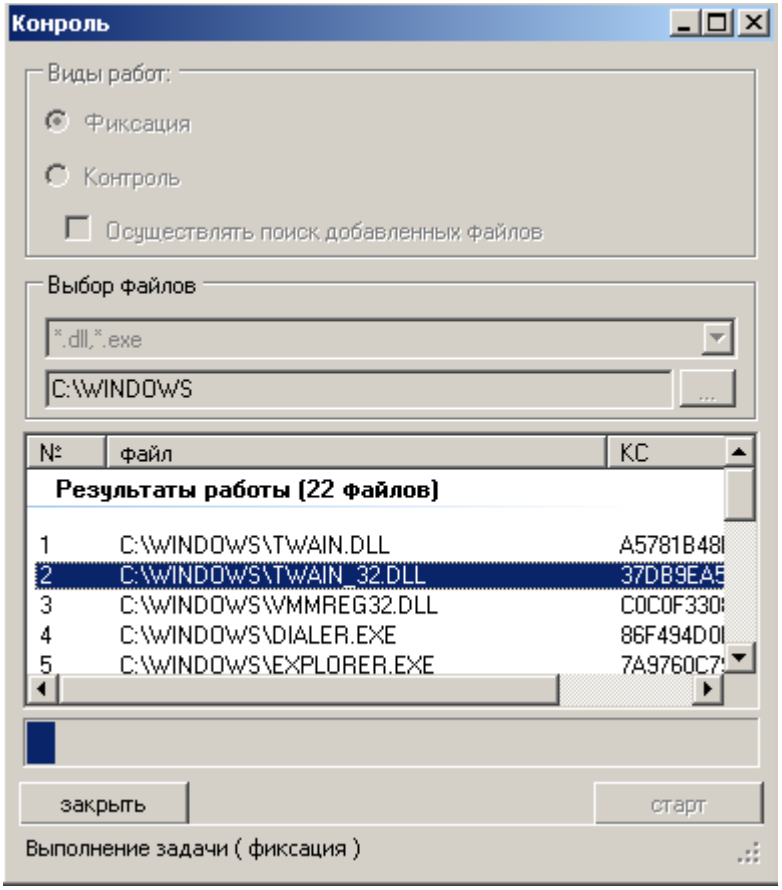


Рисунок 3.14 – Вид окна программы при проведении контроля исходного состояния файлов ОС Microsoft Windows Server 2003

Для проведения контроля исходного состояния необходимо установить переключатель «Вид работы» в положение «Контроль». Для обнаружения в процессе контроля файлов, добавленных в системную папку, необходимо установить флажок «Осуществлять поиск добавленных файлов» и нажать кнопку «Далее». Поле «Выбор файлов» должно содержать такие маски, которые были заданы при проведении фиксации исходного состояния. После нажатия кнопки «Старт» в появившемся диалоговом окне необходимо выбрать имя файла, содержащего результаты фиксации исходного состояния, и нажать кнопку «Открыть». По завершении контроля окно программы будет иметь вид, представленный на рисунке 3.15. В автоматически открывающемся окне будет представлен обобщенный результат контроля – количество проконтролированных файлов, количество измененных файлов, количество отсутствующих файлов, добавленных в системную папку (только при установленном флажке «Осуществлять поиск добавленных файлов).

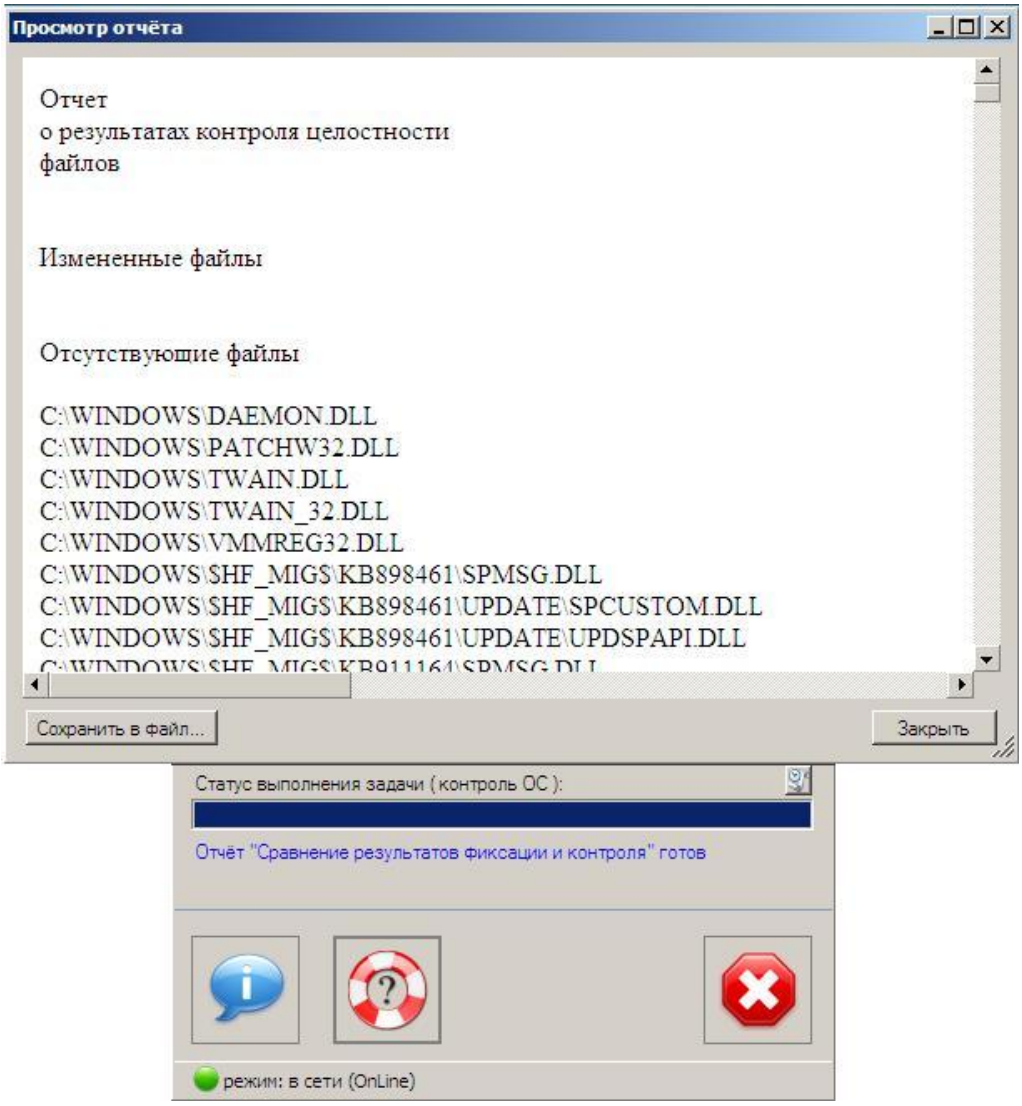


Рисунок 3.15 – Вид окна программы при проведении контроля исходного состояния файлов ОС Microsoft® Windows Server 2003

Проведение контроля целостности рекомендуется проводить при появлении подозрений на вирусы, нарушении исправного функционирования операционной системы, после установки программного обеспечения и т.п.

Создание проекта сертификата соответствия

Для создания проекта Аттестата соответствия необходимо нажать кнопку «Создать проект Аттестата» в главном окне программы. После заполнения необходимых полей, в появившемся окне, вид которого представлен на рисунке 3.16, необходимо нажать кнопку «Далее». Если какое-либо поле останется незаполненным, то в проекте Аттестата в соответствующих местах будет оставлено свободное место для последующего заполнения в редакторе HTML-документов.

Для получения примера заполнения полей необходимо нажать кнопку «Пример». Для очистки полей необходимо нажать кнопку «Сброс». Для формирования проекта Аттестата и записи его в файл в формате HTML необходимо нажать кнопку «Далее».

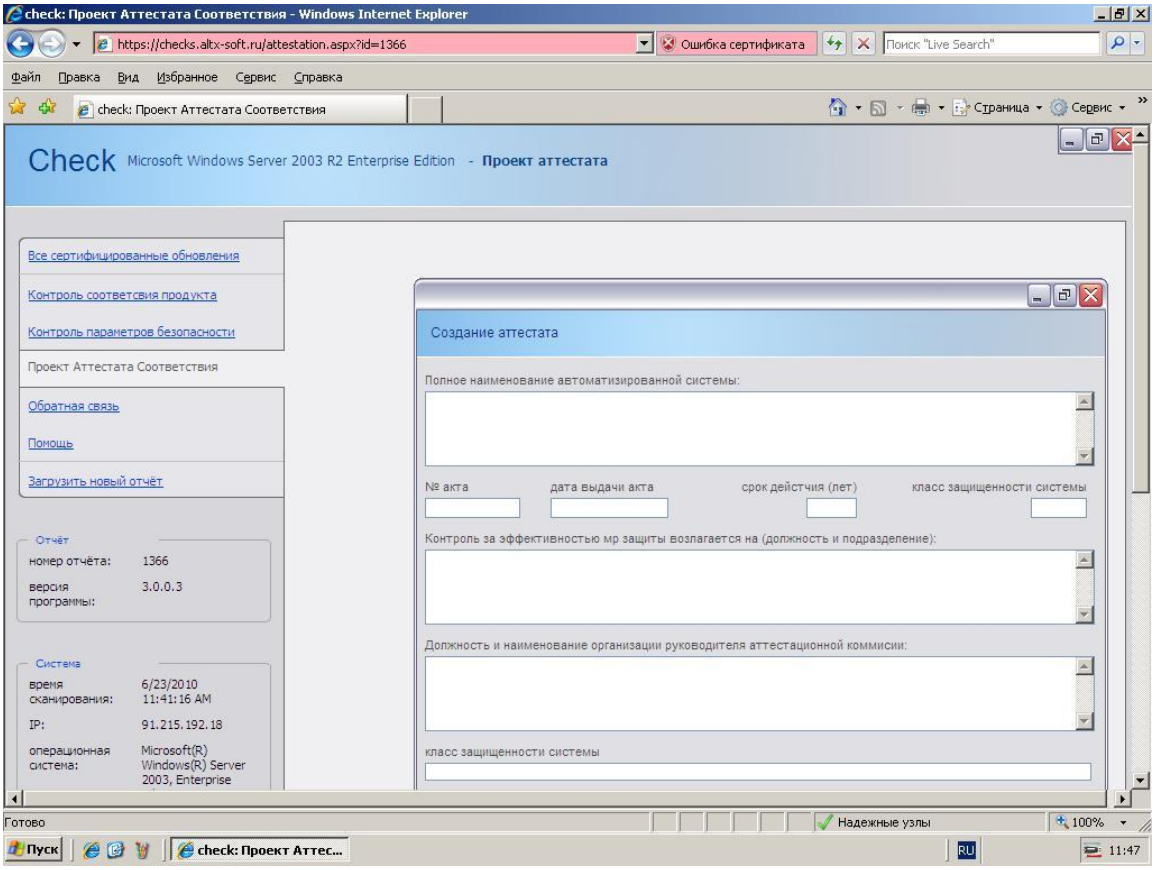


Рисунок 3.16 – Вид окна программы контроля сертифицированной версии Windows Server 2003 в режиме создания проекта Аттестата соответствия после нажатия кнопки «пример»

Для создания проекта Аттестата соответствия с помощью кнопки  на клиентской панели программы, необходимо выполнить функцию *Фиксация и контроль системных файлов Windows*, хотя бы единожды. Изначально, до фиксации, кнопка «Создать проект аттестата соответствия» недоступна пользователю.

Аттестат соответствия можно сгенерировать с защищенного сайта ЗАО «АЛТЭКС-СОФТ», выбрав вкладку «Создать проект аттестата соответствия».

При соответствии файлов сертифицированной ОС Microsoft Windows Server 2003, но несоответствии настроек параметров безопасности контролируемой системы рекомендуемым параметрам, вкладка «отчет о параметрах безопасности», будет иметь вид, представленный на рисунке 3.17.

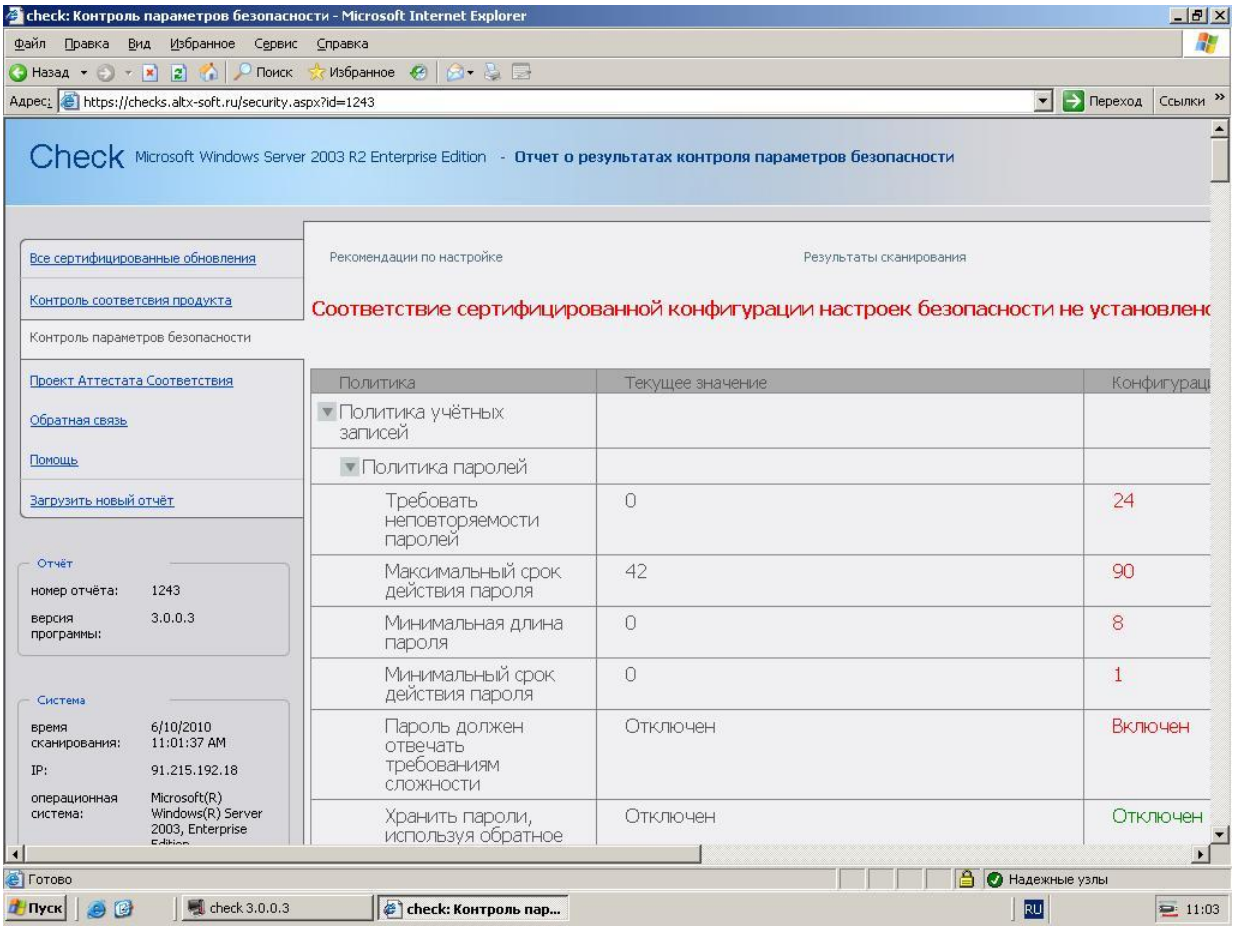


Рисунок 3.17 – Вид окна программы контроля сертифицированной версии Windows Server 2003 при несоответствии настроек параметров безопасности рекомендуемым

3.3 Поиск и диагностика неисправностей программы «Check»

1. *Отсутствует связь с сервером http://check.altx-soft.ru*. Проверьте Ваши настройки сетевого подключения, брандмауэр, антивирусного ПО. Возможно, указанные средства блокирует работу программы контроля, запрещая ей сетевую активность.

2. *Отсутствует или устарел сертификат для доступа в Центр сертифицированных обновлений.* Проверьте наличие электронного сертификата на ключа eToken, входящем в комплект поставки сертифицированного программного обеспечения.

3. *Отсутствует или некорректно установлены сертификаты удостоверяющего центра АЛТЭКС-СОФТ*. Порядок установки сертификатов приведен в Инструкции по организации доступа в Центр сертифицированных обновлений.

Все основные действия программы «Check» записываются в журнал (лог) работы программы (см. рисунок 3.19). При появлении ошибок следует вызвать журнал работы программы (нажать кнопку «Лог работы программы») и передать его содержание, а при

необходимости и скриншоты экранов ошибок в службу технической поддержки ЗАО «АЛТЭКС-СОФТ» support@altx-soft.ru для диагностики неисправности.

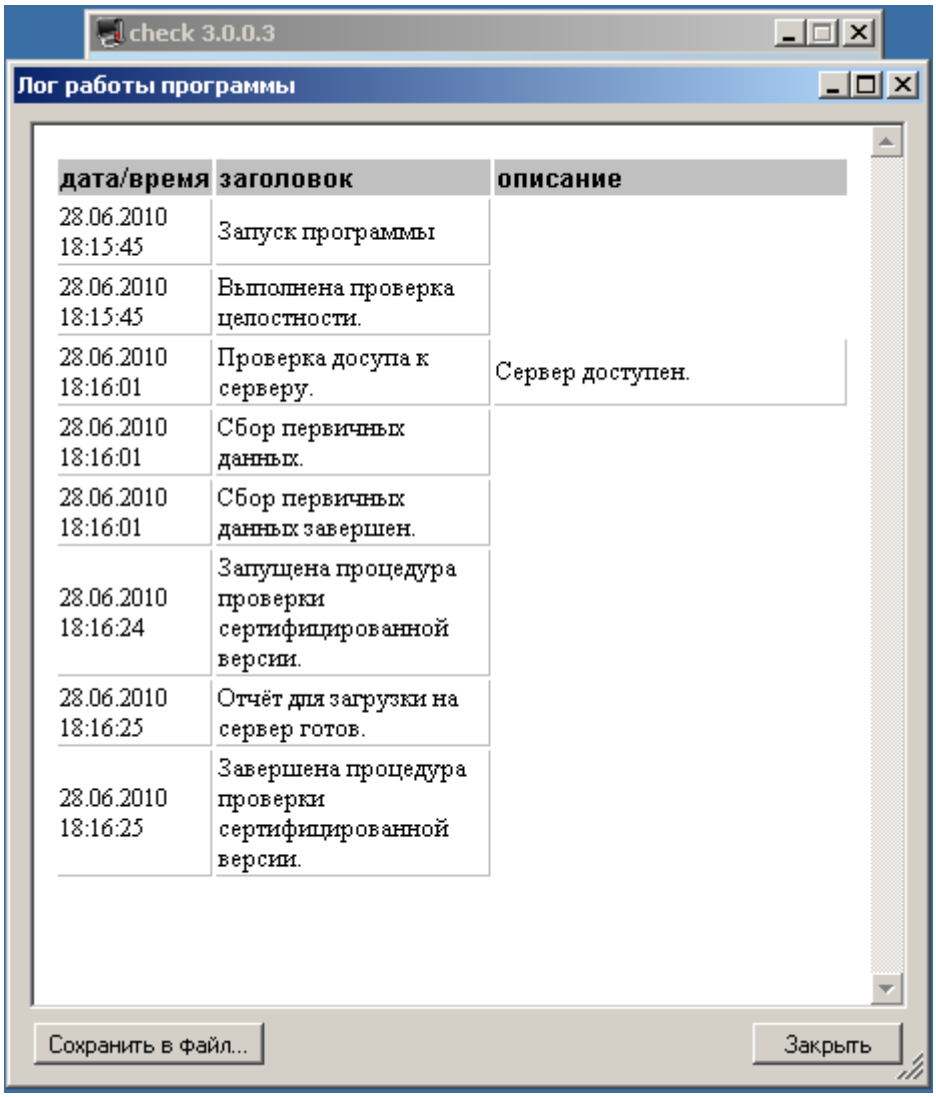


Рисунок 3.19 – Вид информационного окна программы, содержащей техническую информацию, при отсутствии доступа к серверу контроля.

Приложение А

А.1 Групповая политика

Групповая политика представляет собой набор правил, определяющих параметры системы: безопасность, работу приложений и служб, установку программного обеспечения и т.д. Цель политик безопасности – определить процедуры выбора конфигурации и управления безопасностью в среде функционирования. Групповая политика помогает применить технические рекомендации в политике безопасности для всех компьютеров и серверов в доменах Active Directory.

Применение групповой политики осуществляется с целью контроля использования программ, сетевых ресурсов и операционной системы пользователями и компьютерами. Групповые политики позволяют легко и единообразно управлять настройками большого количества вариантов среды серверных компьютерных систем путем выборочного включения и выключения отдельных функций. В случае использования групповой политики для создания настроек безопасности, любые изменения, осуществляемые по отношению к какой-либо из политик, будут относиться ко всем серверам, клиентским компьютерам и пользователям, использующим эту политику.

Существует два типа групповых политик. Первый тип – это локальная групповая политика. Локальная групповая политика может быть только одна, и это единственная групповая политика, доступная на компьютерах, не являющихся членом домена. Она применяется также на всех компьютерах, которые входят в состав домена Active Directory, являясь его участниками.

Второй тип групповой политики – это групповая политика Active Directory. Интегрирование групповой политики со службой каталогов Active Directory позволяет обеспечить большую безопасность и гибкость управления пользователями и объектами сети, позволяя администраторам объединить их в логические группы, такие как организационные подразделения (Organizational Unit), а затем назначать группам единые параметры конфигурации, что обеспечит непротиворечивость их конфигураций. Использование групповой политики в сочетании со структурой организационных подразделений позволяет определять специфические настройки безопасности для тех или иных функций конкретного клиентского компьютера или сервера.

Объекты групповой политики, основанные на Active Directory, фактически состоят из двух разных объектов:

- контейнера групповой политики GPC (Group Policy Container), расположенного в каталоге Active Directory. Данный объект содержит список компонентов,

используемый для определения того, параметры какой группы конфигурационных параметров (относящихся к пользователю или компьютеру) сконфигурированы в данном ОГП, информацию о версии групповой политики и информацию о состоянии, используемую для указания того, является ли ОГП действующим, или он заблокирован;

– шаблона групповой политики GPT (Group Policy Template). Данный объект содержит большинство фактических параметров настройки для групповой политики и расположен в папке совместно используемого ресурса `Sysvol` на каждом контроллере домена.

Шаблоны безопасности

Шаблон безопасности представляет собой текстовый файл, в котором определены параметры безопасности операционной системы Microsoft® Windows Server™ 2003. Каждый шаблон хранить в обычном текстовом файле с расширением `.inf`, что позволяет копировать, импортировать и экспортировать параметры безопасности.

Шаблоны безопасности могут импортироваться как в локальные объекты групповой политики, так и в объекты групповой политики, определяемые в Active Directory. В этом случае все компьютеры и учетные записи пользователей, на которые распространяется групповая политика, применяют конфигурацию безопасности, описанную с помощью данного шаблона. Импорт шаблонов безопасности упрощает администрирование, так как конфигурация безопасности автоматически настраивается сразу для нескольких объектов.

Для изменения шаблонов используется редактор (оснастка) шаблонов безопасности из состава оснасток консоли управления Microsoft Management Console или любой текстовый редактор (например, программа «Блокнот»). Шаблоны безопасности содержат все параметры безопасности, назначаемые объекту групповой политики, кроме относящихся к политикам открытых ключей и политике IPSec. Некоторые разделы шаблона могут содержать списки управления доступом Access Control List (ACL), которые определенны на языке Security Descriptor Definition Language (SDDL).

В таблице А.1.1 показано соответствие между разделами групповой политики и секциями файла шаблона безопасности.

Таблица А.1.1 – Формат шаблона безопасности

Раздел групповой политики	Раздел шаблона безопасности
Политика учетных записей (Account Policy)	[System Access]
Политика аудита (Audit Policy)	[System Log] [Security Log] [Application Log]
Назначение прав пользователя (User Rights Assignment)	[Privilege Rights]
Параметры безопасности (Security Options)	[Registry Values]
Журналы событий (Event Log)	[Event Audit]
Группы с ограниченным доступом (Restricted Groups)	[Group Membership]
Системные службы (System Services)	[Service General Setting]
Реестр (Registry)	[Registry Keys]
Файловая система (File System)	[File Security]

А.2 Параметры безопасности компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003

А.2.1 Описание параметров безопасности, общих для всех рядовых серверов в рамках домена Active Directory

Параметры безопасности, представленные в данном разделе, учитывают особенности конфигураций «Enterprise Client» и «Specialized Security – Limited Functionality». В данном разделе рассматриваются основные параметры безопасности, для настройки которых в домене Active Directory используется групповая политика. Применяемые параметры безопасности являются общими для всех рядовых серверов (**Member Server Baseline Policy**) в рамках домена Active Directory и позволяют обеспечить базовый уровень защищенности (**Baseline Level**) компьютеров. Применение рекомендованных параметров безопасности позволяет защитить информацию, обрабатываемую на компьютерах в организации.

Параметры политики учетных записей

Поскольку политика учетных записей домена определяется в рамках всего домена, она не может быть переопределена любой другой политикой безопасности. Контроллер домена всегда получает политику учетных записей от объекта групповой политики «Default

Domain Policy» (Политика домена, используемая по умолчанию), даже если имеется другая политика учетных записей, примененная к организационному подразделению, которое содержит учетную запись контроллера домена.

При отсутствии политики учетных записей или ее неправильной настройке пользователи получают возможность использования простых форм паролей, не отвечающих требованиям сложности (например, совпадающие с именем входа пользователя), и возможность пользоваться одним и тем же паролем на протяжении неограниченного времени, что дает злоумышленнику возможность организации атак различных типов, направленных на подбор пароля пользователя.

С другой стороны, если настройки политики учетных записей будут чрезмерно жесткими, это приведет к частой смене пользователями своих паролей и увеличению случаев блокирования учетных записей в результате неправильного ввода пароля самими же пользователями. Приведенные далее рекомендации помогут правильно определить оптимальные значения для соответствующих параметров политики учетных записей, к которым относят политику паролей и политику блокировки учетной записи.

Политика паролей

Использование регулярно изменяемых, сложных паролей снижает вероятность их подбора. Параметры политики паролей служат для определения уровня сложности и длительности использования паролей.

Для обеспечения требуемого уровня безопасности с помощью редактора объекта групповой политики необходимо настроить параметры политики паролей в следующем разделе пространства имен ОГП «Default Domain Policy»: `Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей` (см. таблицу А.2.1).

Таблица А.2.1 – Параметры политики паролей, используемые для обеспечения безопасности компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003

Название параметра	**Конфигурация безопасности**	
	Enterprise Client	**Specialized Security – Limited Functionality**
Максимальный срок действия пароля	90 дней	90 дней
Минимальная длина пароля	8 символов	12 символов

Название параметра	Конфигурация безопасности	
	Enterprise Client	Specialized Security – Limited Functionality
Минимальный срок действия пароля	1 день	1 день
Пароль должен отвечать требованиям сложности	Включен	Включен
Хранить пароли, используя обратное шифрование	Отключен	Отключен
Требовать неповторяемости паролей	24 хранимых пароля	24 хранимых пароля

Параметр безопасности «Максимальный срок действия пароля» определяет частоту смены паролей пользователями, а также ограничивает период времени, в течение которого злоумышленник, подобравший пароль пользователя, сможет получать доступ к компьютеру. Значение данного интервала может находиться в диапазоне от 0 до 999 дней.

Подобрать можно практически любой пароль, следовательно, чем чаще пароль изменяется, тем меньше у злоумышленника возможностей им воспользоваться. В то же время, установка слишком низкого значения может привести к резкому росту количества обращений в службу технической поддержки пользователей сети. Установка для трех типов конфигураций безопасности рекомендованного значения параметра «Максимальный срок действия пароля» равным «90 дням» позволит обеспечить регулярность смены пароля, повышая тем самым безопасность его использования.

Параметр безопасности «Минимальная длина пароля» определяет минимальное количество символов пароля. Данный параметр не позволяет использовать пустые пароли, а также пароли, количество символов в которых меньше минимально допустимого.

Увеличение длины пароля на один символ приводит к экспоненциальному повышению сложности его подбора. Например, использование семизначного пароля означает $1x10^7$ возможных комбинаций. С учетом регистра, количество комбинаций (при использовании только символов латинского алфавита) составляет 52^7. Следовательно, 7-символьный пароль, состоящий только из символов алфавита без знаков пунктуации, с учетом регистра имеет 62^7 комбинаций. При скорости 1 000 000 подстановок в секунду для взлома такого пароля потребуется всего 48 минут. 8-символьный пароль означает $2x10^{11}$ комбинаций. При скорости 1 000 000 подстановок в секунду (показатель многих программ для определения паролей), все возможные комбинации будут проверены через 59 часов.

Увеличение длины пароля на один символ также приводит к экспоненциальному повышению его надежности. Использование паролей длиной не менее восьми символов приводит к значительному усилению даже менее надежного механизма хеширования

паролей, как LMHash, поскольку в этом случае злоумышленнику необходимо взломать две части каждого пароля.

В тоже время, применение слишком длинных паролей приводит к учащению ошибок при вводе пароля, увеличению числа заблокированных учетных записей и, как следствие, обращений в службу технической поддержки. Кроме того, использование слишком длинных паролей может привести к фактическому снижению безопасности, поскольку пользователи из боязни забыть пароль вынуждены его записывать.

Исходя их этого, в конфигурации «Enterprise Client» рекомендуемое минимальное значение длина пароля составляет 8 символов. Пароли такой длины позволяют обеспечить соответствующий уровень безопасности и сравнительно легко запоминаются пользователями. В конфигурации безопасности «Specialized Security – Limited Functionality» должны использоваться пароли длинной не менее 12 символов.

Параметр безопасности «Минимальный срок действия пароля» устанавливает длительность периода времени использования пароля до того, как пользователь получит право его сменить. Значение данного параметра может находиться в диапазоне от 1 до 998 дней. При использовании значения равным 0, пользователь получает возможность смены пароля немедленно.

Только при значениях данного параметра, отличных от нуля, обеспечивается эффективность использования параметра безопасности «Требовать неповторяемости паролей». В ином случае пользователь имеет возможность сменить пароль несколько раз подряд, пока не достигнет уже использованного однажды значения. Принятое по умолчанию значение не в полной мере соответствует этой рекомендации, поэтому для трех конфигураций безопасности рекомендуется установить значение параметра «Минимальный срок действия пароля» равным «1 день». Это ограничение не позволит менять пароль чаще одного раза в два дня и, таким образом, препятствует повторному использованию старого пароля пользователями. Кроме того, необходимость использования пароля не менее 1 дня способствует его запоминанию и не дает возможности сразу ввести 24 пароля с целью обхода параметра безопасности «Требовать неповторяемости паролей».

Параметр безопасности «Пароль должен отвечать требованиям сложности» служит для проверки новых паролей на соответствие минимальным базовым требованиям, которые предъявляются к их надежности, а именно:

– пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

- пароль должен состоять не менее чем их шести символов (данное требование переопределяется параметром безопасности «Минимальная длина пароля»);
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:
  - прописные буквы английского алфавита от A до Z;
  - строчные буквы английского алфавита от a до z;
  - десятичные цифры (от 0до 9);
  - неалфавитные символы (например, !, $, &; #, %),

Использование пользователями сложных паролей помогает противостоять атакам на сетевые пароли – как словарным, так и основанным на методе прямого перебора. Словарная атака (dictionary attack) направлена на попытки использовать злоумышленником в качестве пароля либо общеупотребительные слова из орфографического словаря, либо наиболее распространенные пароли и часто используемые словообразования. Атака методом прямого перебора (brute force attack) основана на переборе нарушителем всевозможных комбинации до тех пор, пока одна из них не совпадет с паролем.

Использование пользователями паролей, соответствующих вышеуказанным критериям, позволяет значительно увеличить промежуток времени, который необходим злоумышленнику для осуществления словарных атак. В частности, при использовании 8-символьного пароля, включающего цифры и прописные и строчные символы латинского алфавита, число возможных комбинаций пароля составит $2{,}18 \times 10^{14}$. При скорости 1 000 000 подстановок в секунду все возможные комбинации будут проверены примерно через 7 лет.

Поэтому во всех конфигурациях безопасности данный параметр безопасности должен иметь значение «Включен».

Параметр безопасности «Требовать неповторяемости паролей» определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Эффективность данного параметра обеспечивается использованием параметра «Минимальный срок действия пароля», который предотвращает попытки слишком частого изменения пароля пользователем.

Для трех рассматриваемых конфигураций безопасности рекомендуемое значение данного параметра соответствует «24 хранимых пароля». Установка максимального значения («24 хранимых пароля» является максимально возможным значением) предотвращает повторное (случайное или преднамеренное) использование пользователем пароля, повышая тем самым безопасность системы. Кроме того, утраченные пароли станут

недействительными еще до того, как злоумышленник успеет взломать с их помощью учетную запись пользователя.

Параметр безопасности «Хранить пароли всех пользователей в домене, используя обратимое шифрование» определяет возможность использования операционной системой обратимого шифрования при сохранении паролей. Этот параметр обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранение паролей с использованием обратимого шифрования фактически является альтернативой хранению их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения важнее, чем безопасность пароля. Эта политика является обязательной при использовании протокола аутентификации Challenge-Handshake Authentication Protocol (CHAP) и при использовании проверки подлинности методом Digest Authentication.

Поскольку активация данного параметра приводит к значительному повышению уязвимости операционной системы Microsoft® Windows Server™ 2003, во всех конфигурациях безопасности данную возможность необходимо отключить.

Политика блокировки учетной записи

Политика блокировки, определяет необходимость блокировки учетной записи, если в течение заданного периода времени системой регистрируется определенное количество неудачных попыток входа. Количество неудачных попыток входа в систему и период времени блокировки устанавливаются с помощью параметров политики блокировки учетной записи. Пользователь не сможет войти в систему, если его учетная запись заблокирована, поскольку все попытки входа в систему отслеживаются.

С целью предотвращения возможности подбора пароля злоумышленником и снижения вероятности получения несанкционированного доступа к сети с использованием редактора объектов групповой политики необходимо настроить параметры политики блокировки учетной записи в следующем разделе пространства имен ОГП «Default Domain Policy»: Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика блокировки учетной записи (см. таблицу А.2.2).

Таблица А.2.2 – Параметры политики блокировки учетной записи, используемые для обеспечения безопасности компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003

Название параметра	Конфигурация безопасности	
	Enterprise Client	Specialized Security – Limited Functionality
Время до сброса счётчика блокировки	15 минут	15 минут
Пороговое значение блокировки	50 ошибок входа	10 ошибок входа
Продолжительность блокировки учётной записи	15 минут	15 минут

Параметр безопасности «Блокировка учетной записи на» служит для определения периода времени, по прошествии которого пользователь сможет повторить попытку входа в систему. В течение указанного периода времени учетная запись пользователя будет заблокирован. В случае если значение данного параметра безопасности установлено равным нулю, учетная запись будет недоступна до тех пор, пока администратор вручную не разблокирует ее. Это является хорошей практикой, но может привести к увеличению числа заблокированных учетных записей вследствие ошибок при вводе пароля и, как результат, обращений в службу технической поддержки.

Установка значения параметра «Блокировка учетной записи на» равное «15 минут» в конфигурациии «Enterprise Client» и «15 минут» в конфигурации «Specialized Security – Limited Functionality» обеспечивает достаточную защищенность системы от атак типа «отказ в обслуживании» (при реализации которых злоумышленник может умышленно осуществлять неудачные попытки входа с использованием различных учетных записей пользователей с целью их блокирования системой), не вызывая при этом увеличения количества обращений в службу поддержки пользователей сети.

Параметр безопасности «Пороговое значение блокировки» определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока администратором не будет сброшена блокировка или пока не истечет интервал блокировки. Поскольку уполномоченные пользователи могут заблокировать собственные учетные записи, неправильно введя пароль, то чтобы избежать непреднамеренной блокировки учетных записей необходимо установить высокое пороговое значение блокировки. Для конфигурации безопасности «Enterprise Client» рекомендуется установить значение

блокировки равным «50 ошибок входа в систему», для конфигурации «Specialized Security – Limited Functionality» - равным «10 ошибок входа в систему». Указанные значения позволят избежать частого обращения пользователей в службу поддержки в случае непреднамеренной блокировки ими собственной учетной записи, однако не исключат возможные реализации атак типа «отказ в обслуживании», направленных на преднамеренную блокировку учетных записей.

Параметр безопасности «Сброс счетчика блокировки через» служит для определения периода времени, который должен пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Использование значения по умолчанию или определение слишком длинного интервала делает систему уязвимой перед проведением атаки типа «отказ в обслуживании». Нарушитель может преднамеренно выполнить несколько попыток входа в систему от имени всех пользователей, что приведет к блокировке их учетных записей. Если интервал времени, по прошествии которого выполняется сброс счетчика, не определен, администратору придется разблокировать все учетные записи вручную. С другой стороны, при использовании продуманного значения, учетные записи пользователей будут разблокированы автоматически по истечении заданного периода времени, что уменьшит число обращений в службу поддержки.

Таким образом, для конфигурации безопасности «Enterprise Client» рекомендуется установить значение параметра «Сброс счетчика блокировки через» равным «15 минутам», для конфигурации «Specialized Security – Limited Functionality» - также, равным «15 минутам».

В случае, когда компьютер является автономным компьютером под управлением операционной системы Microsoft® Windows Server™ 2003 в конфигурации «Specialized Security – Limited Functionality», параметры политики учетных записей должны определяться для него отдельно от существующей в домене политики учетных записей пользователей.

Параметры локальной политики

Параметры локальной политики должны быть настроены централизованно для всего множества компьютеров, функционирующих в заданной конфигурации безопасности. Для этого используется объекты групповой политики, базирующиеся на основе службы каталогов Active Directory. К параметрам локальной политики относят политику аудита, назначение прав пользователям и параметры безопасности.

Параметры политики аудита

Параметры политики аудита определяют категории событий безопасности, которые отслеживаются системой и включаются в соответствующий отчет. В результате этого создается журнал регистрации определенных действий самой системы и пользователей (далее – журнал регистрации событий безопасности). Таким образом, администратор получает возможность отслеживать действия, относящиеся к безопасности, например, доступ к контролируемому объекту, вход/выход пользователя в/из системы, а также изменения параметров политики аудита.

Перед внедрением политики аудита необходимо определить категории событий, которые будут отслеживаться системой. Политика аудита определяется выбранными для каждой категории событий параметрами. Путем определения параметров для различных категорий событий можно создавать политику аудита, удовлетворяющую всем требованиям безопасности организации.

Если политика аудита не настроена, то в случае возникновения нарушений, связанных с безопасностью, будет сложно (или невозможно) определить сущность, источник и другие параметры нарушений. С другой стороны, если подсистема аудита отслеживает большое количество событий аудита, журнал регистрации событий безопасности будет переполнен бесполезной информацией. Приведенные далее рекомендации помогут взвешенно подойти к определению отслеживаемых действий и метода сбора данных аудита.

С помощью редактора групповой политики необходимо настроить параметры политики аудита в следующем разделе пространства имен объекта групповой политики: `Конфигурация компьютера\Конфигурация Windows\Параметры безопасности \Локальные политики\Политика аудита` (см. таблицу А.2.3).

Таблица А.2.3 – Параметры политики аудита, используемые для обеспечения безопасности компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003

Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security –
Аудит входа в систему	Успех	Успех, Отказ
Аудит изменения политики	Успех	Успех
Аудит системных событий	Успех	Успех
Аудит событий входа в систему	Успех	Успех, Отказ

Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security –
Аудит управления учетными записями	Успех	Успех, Отказ
Аудит использования привилегий	Не определено	Отказ
Аудит доступа к службе каталогов	Не определено	Отказ

Параметр «Аудит событий входа в систему» используется для определения, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на другом компьютере, при условии, что обработка запроса на проверку правильности учетной записи пользователя осуществляется компьютером, ведущим журнал регистрации событий. Таким образом, события, контролируемые параметром «Аудит событий входа в систему» заносятся в журнал на том компьютере, где хранится учетная запись пользователя.

Этот параметр позволяет вести учет успешных и неудавшихся попыток входа пользователей в систему. Параметр позволяет администратору определять системы в сети, доступ к которым был получен с компьютера под управлением операционной системе Microsoft® Windows Server™ 2003. Для конфигурации «Enterprise», параметр «Аудит событий входа в систему» должен иметь значение «Успех», а для «Specialized Security – Limited Functionality» - «Успех, Отказ».

Параметр «Аудит управления учетными записями» используется для отслеживания попыток создания новых пользователей и групп, переименования пользователей и групп, активации и деактивации учетных записей пользователей, изменения пароля учетных записей, а также включения аудита событий управления учетными записями.

Активация этого параметра политики аудита позволяет администратору контролировать злонамеренное, случайное и санкционированное создание учетных записей пользователей и групп. Для конфигурации «Enterprise», параметр «Аудит управления учетными записями» должен иметь значение «Успех», а для «Specialized Security – Limited Functionality» - «Успех, отказ».

Параметр «Аудит доступа к службе каталогов» может быть активирован только на контроллерах домена. По этой причине на уровне рабочих станций он не определяется.

Параметр «Аудит входа в систему» используется для отслеживания успешных и неудавшихся попыток входа в систему следующих типов: интерактивный вход, сетевой вход, вход в качестве службы и вход в качестве пакетного задания. События, контролируемые параметром «Аудит входа в систему», заносятся в журнал регистрации событий на том компьютере, где сделана попытка войти в систему.

Этот параметр позволяет администратору контролировать перечисленные события и вести учет успешных и неудавшихся попыток входа в компьютеры под управлением операционной системы Microsoft® Windows Server™ 2003. Для конфигурации «Enterprise», параметр «Аудит управления учетными записями» должен иметь значение «Успех», а для «Specialized Security – Limited Functionality» - «Успех, отказ».

Параметр «Аудит изменения политики» служит для отслеживания изменений прав пользователей и политики аудита. Настройка данного параметра позволяет администратору подтверждать санкционированные изменения и выявлять несанкционированные. Все изменения прав пользователей или политики аудита записываются в виде событий в журнал регистрации событий.

Для конфигурации «Enterprise» и «Specialized Security – Limited Functionality» параметр «Аудит управления учетными записями» должен иметь значение «Успех».

Параметр «Аудит использования привилегий» позволяет отслеживать действия, для выполнения которых требуется использование предоставленных учетной записи пользователя особых привилегий. При их использовании соответствующие события будут записаны в журнал регистрации событий. Кроме того, этот параметр используется для учета попыток создания резервных копий и восстановления файлов или папок с помощью соответствующих прав пользователя. Однако эти события будут фиксироваться только в том случае, если активирован параметр безопасности для отслеживания попыток создания резервных копий и восстановления.

Данный параметр должен быть активирован для конфигурации безопасности «Specialized Security – Limited Functionality». При этом рекомендуется осуществлять аудит только неуспешных попыток использования привилегий, поскольку при аудите успешных попыток в журнале безопасности будет регистрироваться значительное количество записей аудит, что в свою очередь приведет к его быстрому переполнению.

Параметр «Аудит системных событий» позволяет отслеживать успешные и неудачные системные события для выявления случаев несанкционированного доступа к системе. К числу системных событий относятся запуск и выключение компьютеров,

переполнение журналов регистрации событий, и прочие, имеющие отношение к безопасности события, которые оказывают влияние на систему в целом.

По этой причине в конфигурациях «Enterprise» и «Specialized Security – Limited Functionality» параметр «Аудит системных событий» должен иметь значение «Успех».

Параметры назначения прав пользователей

Задачи, которые пользователь имеет право выполнять в домене или в операционной системе, установленной на компьютере, называются правами пользователя. Существует два типа прав: права, связанные с входом в систему, и привилегии. Права, связанные с входом в систему, определяют, кто и как имеет право входить в систему на конкретном компьютере. С помощью привилегий контролируется доступ с данного компьютера ко всем ресурсам системы, причем привилегии могут переопределять разрешения, установленные для отдельных объектов.

Приведенные далее рекомендации помогут правильно определить оптимальные значения для соответствующих параметров назначений прав пользователя (см. таблицу А.2.4).

В операционной системе Microsoft® Windows Server™ 2003 параметры назначения прав пользователей следует настраивать в редакторе групповой политики в следующем разделе пространства имен объекта групповой политики: Конфигурация компьютера\ Конфигурация Windows\Параметры безопасности\Локальные политики\ Назначение прав пользователей.

Таблица А.2.4 – Параметры назначения прав пользователей, используемые для обеспечения безопасности компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
1.	Доступ к компьютеру из сети	Не задано	Группа: контроллеры домена предприятия Все пользователи, прошедшие проверку (гость в эту группу не входит)

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
			Группа: администраторы
2.	Работа в режиме операционной системы	Не задано	Никто
3.	Настройка квот памяти для процесса	Не задано	Локальная служба 'LOCAL SERVICE' Сетевая служба 'NETWORK SERVICE' Группа: администраторы
4.	Локальный вход в систему	Группа: администраторы Группа: опытные пользователи Группа: операторы архива	Группа: администраторы
5.	Разрешать вход в систему через службу терминалов	Группа: администраторы Группа: пользователи удаленного рабочего стола	Группа: администраторы
6.	Архивирование файлов и каталогов	Не задано	Группа: администраторы
7.	Обход перекрестной проверки	Не задано	Все пользователи, прошедшие проверку (гость в эту группу не входит)
8.	Изменение системного времени	Не задано	Локальная служба 'LOCAL SERVICE' Группа: администраторы
9.	Создание страничного файла (pagefile)	Не задано	Группа: администраторы
10.	Отладка программ	Группа: администраторы	Не задано
11.	Создание маркерного объекта	Не задано	Никто

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
12.	Создание объектов в глобальном пространстве имён	Не задано	Группа: все участники безопасности, вошедшие в систему в качестве службы. Принадлежность контролируется операционной системой(СЛУЖБА) Группа: администраторы
13.	Создание постоянных объектов совместного использования	Не задано	Никто
14.	Отказ в доступе к этому компьютеру из сети	Группа: гости АНОНИМНЫЙ ВХОД	Группа: гости АНОНИМНЫЙ ВХОД
15.	Отказ во входе в качестве пакетного задания	Группа: гости	Группа: гости
16.	Отклонить локальный вход	Не задано	Группа: гости
17.	Запретить вход в систему через службу терминалов	Группа: гости	Группа: гости
18.	Разрешение доверия к учетным записям при делегировании	Не задано	Группа: администраторы
19.	Принудительное удаленное завершение	Не задано	Группа: администраторы
20.	Создание журналов безопасности	Не задано	Локальная служба 'LOCAL SERVICE' Сетевая служба 'NETWORK SERVICE'
21.	Управление аудитом и журналом безопасности	Не задано	Группа: администраторы

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
22.	Олицетворение клиента после проверки подлинности	Не задано	Группа: все участники безопасности, вошедшие в систему в качестве службы. Принадлежность контролируется операционной системой(СЛУЖБА) Группа: администраторы
23.	Увеличение приоритета диспетчирования	Не задано	Группа: администраторы
24.	Загрузка и выгрузка драйверов устройств	Не задано	Группа: администраторы
25.	Закрепление страниц в памяти	Не задано	Никто
26.	Изменение параметров среды оборудования	Не задано	Группа: администраторы
27.	Запуск операций по обслуживанию тома	Не задано	Группа: администраторы
28.	Профилирование одного процесса	Не задано	Группа: администраторы
29.	Профилирование загруженности системы	Не задано	Группа: администраторы
30.	Извлечение компьютера из стыковочного узла	Не задано	Группа: администраторы
31.	Замена маркера уровня процесса	Не задано	Локальная служба 'LOCAL SERVICE' Сетевая служба 'NETWORK SERVICE'
32.	Восстановление файлов и каталогов	Не задано	Группа: администраторы
33.	Завершение работы системы	Не задано	Группа: администраторы
34.	Овладение файлами или иными объектами	Не задано	Группа: администраторы

Параметр «Доступ к компьютеру из сети» определяет категории пользователей, которым предоставлено право подключения к данному компьютеру по сети.

Это право необходимо при работе с рядом сетевых протоколов, включая протоколы SMB (Server Message Block), NetBIOS (Network Basic Input/Output System), CIFS (Common Internet File System), HTTP (Hypertext Transfer Protocol) и COM+ (Component Object Model Plus).

Пользователи, работающие на подключенном к сети компьютере, могут иметь доступ к открытым для них сетевым ресурсам. В свою очередь некоторые программы автоматически добавляют к списку учетных записей пользователей, которым предоставлено данное право, группу «Все». При наличии такой группы доступ к компьютерам сети смогут иметь анонимные пользователи, наряду с теми, кто прошел процедуры идентификации и аутентификации. Чтобы не допустить этого, в конфигурации «Specialized Security – Limited Functionality» данное право следует предоставить группам «Контроллеры домена предприятия»,«Администраторы» и «Все пользователи прошедшие проверку».

Право «Работа в режиме операционной системы» разрешает процессу проходить проверку подлинности как обычному пользователю, выступая в последствии от его имени, и таким образом получать доступ к тем же ресурсам, что и любой пользователь. Эта привилегия требуется только для служб проверки подлинности низкого уровня.

Потенциально доступ не ограничен ресурсами, назначенными пользователю по умолчанию, поскольку для процесса вызова может потребоваться, чтобы в описатель доступа были внесены еще какие-либо разрешения. Более важным является тот фактор, что процесс вызова может создать анонимный описатель, способный поддержать любые разрешения на доступ. Кроме того, этот описатель не может служить уникальным идентификатором при отслеживании событий в журнале аудита. По этим причинам, в конфигурации безопасности «Specialized Security – Limited Functionality» указанной привилегией не должен обладать никто.

Параметр «Настройка квот памяти для процесса» определяет, какие учетные записи могут использовать процесс, обладающий разрешением «Запись свойства» для доступа к другому процессу, с целью увеличить назначенную последнему квоту ресурсов процессора. Данная привилегия используется для настройки системы, но ее использование может вызвать неблагоприятные последствия, например, в случае атаки типа «отказ в обслуживании» (Denial of Service).

Исходя из этого, в конфигурации «Specialized Security – Limited Functionality» право «Настройка квот памяти для процесса» необходимо предоставить только группе «Администраторы», «Локальная служба» (Local Service) и «Сетевая служба» (Network Service).

Право «Локальный вход в систему» определяет перечень пользователей, которые могут осуществлять интерактивный вход в систему. Оно также необходимо при входе в систему с помощью службы терминалов или службы Internet Information Service (IIS). Учетная запись с правом локального входа в систему позволяет использовать для входа консоль компьютера. Если предоставить это право группе «Все», то помимо пользователей, обладающих действительными учетными записями, вход в систему может быть выполнен несанкционированным пользователем, с целью загрузить и выполнить злонамеренную программу для получения более высоких привилегий.

Исходя из этого, в конфигурации «Enterprise» это право необходимо предоставить только группе «Администраторы», а в конфигурации «Specialized Security – Limited Functionality» - группам «Администраторы», «Опытные пользователи» и «Операторы архива».

Параметр «Разрешать вход в систему через службу терминалов» предоставляет соответствующим пользователям и членам групп входить в систему в качестве клиента службы терминалов. При использовании «Удаленного помощника» корпоративной службой поддержки необходимо создать соответствующую группу и предоставить ей с помощью групповой политики право входа в систему через службу терминалов. Если служба поддержки в организации не использует возможности «Удаленного помощника», данное право необходимо предоставить только группе «Администраторы», что позволит ограничить возможность доступа к компьютерам с использованием «Удаленного помощника» нежелательных пользователей. Кроме того, необходимо воспользоваться таким средством, как группы с ограниченным доступом, для обеспечения отсутствия в составе группы безопасности «Пользователи удаленного рабочего стола» учетных записей каких-либо пользователей.

Исходя из этого, в конфигурации «Specialized Security – Limited Functionality» право «Разрешать вход в систему через службы терминалов» необходимо предоставить только группе «Администраторы», а в конфигурации «Enterprise» - группам «Администраторы» и «Пользователи удаленного рабочего стола».

Параметр «Архивирование файлов и каталогов» предоставляет соответствующим пользователям обходить ограничения на доступ к файлам и каталогам при создании архивной копии системы. Это право действует только тогда, когда приложение обращается к файлам и каталогам посредством интерфейса API для архивирования

файловой системы NTFS, как например программа NTBACKUP.EXE. В противном случае применяются обычные разрешения на доступ к файлам и каталогам.

В конфигурации «Specialized Security – Limited Functionality», данное право, определяющее границы доступа к файлам и папкам на клиентских компьютерах, необходимо предоставить только локальной группе «Администраторы».

Параметр «Обход перекрестной проверки» в конфигурации «Specialized Security – Limited Functionality», должен быть предоставлен всем пользователям, прошедшим проверку (Гость в эту группу не входит).

Параметр «Изменение системного времени» предоставляет пользователям право изменять время и дату на внутренних часах компьютеров. Действия пользователей, обладающих таким правом, могут повлиять на отображение записей в журналах регистрации событий. Изменение системного времени приводит к тому, что записанным событиям соответствует новое время, а не время их действительного возникновения. Кроме того, несоответствие между временами, установленными на локальном компьютере и на контроллерах домена, может вызвать проблемы в работе протокола проверки подлинности Kerberos, в результате чего пользователи не смогут подключиться к домену или получить права на доступ к ресурсам домена после входа в сеть. Вследствие этого, в конфигурации «Specialized Security – Limited Functionality» данным правом должны обладать только члены группы «Администраторы» и «Локальная служба 'LOCAL SERVICE'».

Параметр «Создание страничного файла» определяет возможность создания пользователем, обладающим данным правом, страничного файла и изменения его размера. Создавая файл подкачки значительного размера, или делая его очень маленьким, злоумышленник может влиять на производительность системы.

Исходя из этого, в конфигурации «Specialized Security – Limited Functionality» данное право должно быть предоставлено только группе безопасности «Администраторы».

Параметр «Создание постоянных объектов совместного использования» определяет, какие учетные записи могут использоваться процессами для создания объекта каталога в диспетчере объектов системы. Это означает, что пользователь, обладающий данной привилегией, сможет создавать общие папки, принтера и другие объекты. Данная привилегия необходима для компонентов режима ядра, которые расширяют пространство имен объектов. Поскольку компоненты, работающие в режиме ядра, уже обладают этой привилегией, им не нужно специально назначать ее.

Исходя из этого, в конфигурации «Specialized Security – Limited Functionality» данное право не должно быть предоставлено никому (значение «No One» – Никто).

Параметр «Создание маркерного объекта» определяет, какие учетные записи могут использоваться процессами для создания маркера доступа, позволяющего получать доступ к локальным ресурсам. В средах, в которых предъявляются высокие требования к безопасности, данное право не должно быть предоставлено никому. Процессам, которым необходима данная привилегия, рекомендуется использовать учетную запись «Локальная система» (Local System), уже включающую данную привилегию, а не отдельную учетную запись пользователя, специально назначая ей эту привилегию.

Исходя из этого, в конфигурации «Specialized Security – Limited Functionality» использование данной привилегии должно быть запрещено для всех (значение «No One» – Никто).

Параметр «Отладка программ» предоставляет пользователя право вызывать отладчик для работы с любым процессом или ядром. Данное право не требуется разработчикам, которые отлаживают приложения, запускаемые в рамках их собственной пользовательской учетной записи. Однако разработчикам, отлаживающим системные компоненты или приложения, запускаемые в рамках других учетных записей, такое право необходимо. Данное право обеспечивает пользователям доступ к самым важным компонентам операционной системы. При отладке можно получить точные сведения о системе из системной памяти. Некоторые средства несанкционированного доступа используют право на отладку программ для извлечения хешированных паролей и других сведений, критичных для безопасности. Для минимизации риска в конфигурации «Enterprise» данной привилегией должны обладать только участники группы безопасности «Администраторы».

Назначение права «Отказ в доступе к компьютеру из сети» означает для пользователей запрет на доступ к данному компьютеру через сеть. Данный параметр имеет больший приоритет по сравнению с параметром «Доступ к компьютеру из сети», если учетная запись пользователя контролируется обеими политиками. В средах, в которых предъявляются высокие требования к безопасности, удаленный доступ пользователей к рабочим станциям должен быть блокирован. Для обеспечения контролируемого доступа к совместно используемым ресурсам должны быть использованы файловые сервера.

В связи с этим, в обеих конфигурациях доступ к рабочим станциям из сети наряду с анонимными пользователями, должны быть лишены пользователи группы «Гость».

Параметр «Отклонить локальный вход» определяет, каким пользователям запрещается интерактивный вход в систему на данном компьютере с консоли. Если злоумышленнику разрешен интерактивный вход в ОС на заданном компьютере, то он

обладает потенциальной возможностью загрузки злонамеренного кода и, таким образом, повышения собственных полномочий в системе. Кроме того, с этим связано наличие других угроз безопасности. Таким образом, данное право должно быть предоставлено только тем категориям пользователей, которые осуществляют интерактивную регистрацию в системе. Данная политика отменяет политику «Локальный вход в систему», если учетная запись пользователя контролируется обеими политиками.

Исходя из этого, в конфигурации безопасности «Specialized Security – Limited Functionality» интерактивный локальных вход в систему должен быть запрещен с использованием учетной записи группы «Гость».

Назначение права «Запретить вход в систему через службу терминалов» означает для пользователей запрет на подключение к компьютерам с помощью удаленного рабочего стола. Введение запрета на подключение к компьютерам через службы терминалов для группы «Все» означает распространение этого запрета и на определенную по умолчанию группу «Администраторы». Поэтому право «Запретить вход в систему через службу терминалов» в конфигурациях «Enterprise» и «Specialized Security – Limited Functionality» должно быть предоставлено группе «Гости».

Параметр «Разрешение доверия к учетным записям при делегировании» определяет, какие пользователи обладают полномочиями по управлению атрибутом «Доверен для делегирования» в отношении объектов «пользователь» или «компьютер» каталога Active Directory. Серверный процесс, который работает на компьютере (или в контексте безопасности пользователя), доверенном для делегирования, может получать доступ к ресурсам другого компьютера, используя делегированные учетные данные клиента, при условии, что для учетной записи клиента не установлен атрибут «Учетная запись важна и не может быть делегирована». Таким образом, наличие у злоумышленника данной привилегии может позволить ему выступать от имени (имперсонировать) другого пользователя при доступе к защищаемым ресурсам.

Исходя из этого, в конфигурации безопасности «Specialized Security – Limited Functionality» использование данной привилегии должно быть предоставлено группе «Администраторы».

Право «Принудительное удаленное завершение» дает возможность пользователям дистанционно по сети отключать компьютеры под управлением операционной системы Microsoft® Windows Server™ 2003. Так как любой пользователь, имеющий право на отключение компьютера, может спровоцировать атаку типа «отказ в

обслуживании» – ситуацию, при которой компьютер не может обслуживать запросы пользователей, то в связи с этим данное право рекомендуется предоставлять только группе «Администраторы».

Поэтому право «Принудительное удаленное завершение» в конфигурации «Specialized Security – Limited Functionality» должно быть предоставлено только группе «Администраторы», а в конфигурации «Enterprise» значение для данного параметра может быть не задано.

Право «Создание журналов безопасности» определяет, какие пользователи или процессы могут осуществлять запись данных аудита в журнал безопасности операционной системы. В случае, если злоумышленник обладает данной привилегией, это позволит ему регистрировать в журнале безопасности значительное количество записей аудита с целью его переполнения или скрытия каких-либо несанкционированных действий.

Поэтому право «Создание журналов безопасности» в конфигурации «Specialized Security – Limited Functionality» должно быть предоставлено только учетным записям «Локальная служба» и «Сетевая служба».

Наличие у пользователя права «Увеличение приоритета диспетчирования» предоставляет ему разрешение «Запись свойства» для доступа к процессам, что в свою очередь определяет возможность управления пользователем приоритетом выполнения процессов. По этой причине, злоумышленник, обладающий данным правом, имеет возможность увеличить приоритет заданного процесса до уровня «реального времени», создав тем самым предпосылки для реализации атаки «отказ в обслуживании».

Исходя из этого, в конфигурации «Specialized Security – Limited Functionality» использование данной привилегии должно быть ограничено только участниками группы безопасности «Администраторы».

Право «Загрузка и выгрузка драйверов устройств» определяет, какие пользователи могут динамически загружать и выгружать драйверы устройств. Данная привилегия необходима для установки драйверов устройств «Plug and Play». Наличие данного права у злоумышленника, позволит ему выполнить загрузку злонамеренного кода под видом драйвера устройства и в последствии реализовать атаку «повышение привилегий». Данное право, наряду с членством в группе безопасности «Администраторы», должно быть предоставлено пользователям, выполняющим установку принтеров и инсталляцию драйверов.

Таким образом, для реализации повышенных требований к безопасности, в конфигурации «Specialized Security – Limited Functionality» право «Загрузка и выгрузка

драйверов устройств» должно быть предоставлено только участникам группы безопасности «Администраторы».

Наличие права «Отказ во входе в качестве пакетного задания» не позволяет пользователю входить в систему с помощью средства обработки пакетных заданий (планировщика заданий). Планировщик заданий часто используется в административных целях, однако его использование должно быть ограничено в средах с высокими требованиями к безопасности, что позволит предотвратить неправильное использование системных ресурсов или запуск злонамеренного кода.

Исходя из этого, в конфигурациях безопасности «Enterprise» и «Specialized Security – Limited Functionality» использование данного права должно быть ограничено только для группы «Гости» и пользователей выполнивших Анонимный вход.

Право «Управление аудитом и журналом безопасности» определяет, какие пользователи могут задавать параметры аудита доступа к объектам для отдельных ресурсов, таких как файлы, объекты Active Directory и разделы реестра, а также очистку журнала безопасности. Поскольку данное право позволяет пользователям управлять журналом безопасности и аудитом для всей системы в целом, в конфигурации «Specialized Security – Limited Functionality» оно должно быть предоставлено только участникам группы безопасности «Администраторы».

Право «Изменение параметров среды оборудования» определяет, каким группам безопасности и пользователям разрешено изменять значения общесистемных параметров среды. Данная информации обычно храниться в разделе реестра «Последняя удачная конфигурация» (Last Known Good Configuration). Модификация данных параметров может привести к сбоям аппаратного обеспечения и создать предпосылки для реализации атаки «отказ в обслуживании». Поэтому в конфигурации «Specialized Security – Limited Functionality» данное право должно быть предоставлено только участникам группы безопасности «Администраторы».

Право «Запуск операций по обслуживанию тома» предоставляет пользователям полномочия на выполнение процедур обслуживания дисковых томов, таких как очистка, дефрагментация и управление всей конфигурацией диска. Наличие у пользователя данного права позволяет ему удалять тома на диске, что приводит к уничтожению содержащихся на них данных.

Исходя из этого, в конфигурации «Specialized Security – Limited Functionality» использование данной привилегии должно быть ограничено только участниками группы безопасности «Администраторы».

Пользователи, которым предоставлено право «Профилирование одного процесса», могут использовать средства для контроля за производительностью несистемных процессов. Для использования оснастки «Системный монитор», как правило, не требуется специально предоставлять данное право. Однако в этом может возникнуть необходимость, если служба «Системный монитор» осуществляет сбор данных с помощью инструментария управления Windows WMI (Windows Management Instrumentation). Ввод ограничений на использование данного права позволяет избежать несанкционированного получения дополнительных сведений, которые могут быть использованы для организации атаки на систему. Кроме того, нарушитель сможет определить, какие процессы запущены в системе и какие пользователи в данный момент работают в ней, и принять меры для обхода таких средств защиты, как антивирусная программа или система обнаружения вторжений.

Поэтому право «Профилирование одного процесса» в конфигурации «Specialized Security – Limited Functionality» должно быть предоставлено группе «Администраторы».

Право «Профилирование загруженности системы» определяет возможность наблюдения пользователями за рабочими характеристиками системных процессов. В свою очередь данное право может быть использовано злоумышленником для определения того, какие процессы запущены в системе, что в дальнейшем послужит ему базисом для организации различных атак.

Поэтому данное право в конфигурации «Specialized Security – Limited Functionality» должно быть предоставлено группе «Администраторы».

Право «Замена маркера уровня процесса» определяет возможность инициирования пользователями процесса замены стандартного маркера доступа, ассоциированного с запущенным дочерним процессом (подпроцессом). Данное право может быть использовано с целью изменения маркера доступа подпроцесса, что приведет к изменению контекста безопасности и повышению его привилегий.

Возможность использования права «Замена маркера уровня процесса» в конфигурации безопасности «Specialized Security – Limited Functionality» должна быть ограничена учетными записями «Локальная служба» и «Сетевая служба».

Пользователи, обладающие правом «Восстановление файлов и каталогов», могут игнорировать разрешения, установленные для файлов, каталогов и других постоянных объектов, при восстановлении архивированных файлов и каталогов на компьютерах под управлением операционной системы Microsoft® Windows Server™ 2003 R2. Кроме того, это право дает возможность пользователям назначать действующих участников безопасности

(security principal) владельцами объектов. По своему характеру данное право аналогично праву «Архивирование файлов и каталогов».

Данное право в конфигурации «Specialized Security – Limited Functionality» должно быть предоставлено группе «Администраторы», а в конфигурации «Enterprise» значение для данного параметра может быть «не задано».

Пользователи, которым предоставлено право «Завершение работы системы», могут с помощью одноименной команды завершать работу операционной системы при интерактивной работе на компьютере. Неправильное назначение данного права может привести к отказу в обслуживании. Исходя из этого, данное право в конфигурации «Specialized Security – Limited Functionality» должно быть предоставлено группе «Администраторы».

Право «Овладение файлами или иными объектами» определяет возможность становления пользователем владельцем любого объекта системы, контролируемого средствами безопасности, в том числе объектов каталога Active Directory, файлов и папок, принтеров, разделов реестра, процессов и их потоков. Наличие данного права позволяет пользователю, обладающего им, действовать в обход прав доступа, установленных на объекте доступа и становиться его владельцем.

В конфигурации «Specialized Security – Limited Functionality» данное право должно быть предоставлено группе «Администраторы».

В домене Active Directory каждая учетная запись компьютера является полноценным участником безопасности с правом проверки подлинности и получения доступа к ресурсам домена. В некоторых случаях количество компьютеров в составе домена Active Directory должно строго контролироваться и быть ограничено. В таких ситуациях предоставление пользователям права добавлять рабочие станции к домену нецелесообразно. Кроме того, наличие данного права позволяет пользователям выполнять действия, которые сложно отследить. Исходя из этого в двух конфигурациях безопасности данное право должно быть предоставлено только группе «Администраторы».

Параметры безопасности

Данные параметры позволяют включать и отключать параметры безопасности компьютера и по существу позволяют пользователям операционной системы Microsoft® Windows Server™ 2003 изменять параметры системного реестра, влияющие на безопасность, без непосредственного редактирования самого реестра. Они позволяют определить

дополнительные характеристики, определяющие поведение системы, и в основном требуются только при повышении уровня ее защищенности.

С помощью редактора групповой политики необходимо настроить параметры безопасности операционной системы Microsoft® Windows Server™ 2003, представленные в таблице А.2.5. Параметры безопасности следует настраивать в редакторе групповой политики в следующем разделе пространства имен объекта групповой политики: `Конфигурация компьютера\Конфигурация Windows\Параметры безопасности \Локальные политики\Параметры безопасности.`

Таблица А.2.5 – Параметры, используемые для обеспечения безопасности компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
1.	Учетные записи: ограничить использование пустых паролей только для консольного входа	Включен	Включен
2.	Аудит: аудит доступа глобальных системных объектов	Отключен	Отключен
3.	Аудит: аудит прав на архивацию и восстановление	Отключен	Отключен
4.	Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности	Отключен	Отключен
5.	Устройства: разрешать отстыковку без входа в систему (laptop)	Отключен	Отключен
6.	Устройства: разрешено форматировать и извлекать съемные носители	Администраторы	Администраторы
7.	Устройства: запретить пользователям установку драйверов принтера	Включен	Включен
8.	Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям	Не определено	Отключен
9.	Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям	Не определено	Отключен

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
10	Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала	Включен	Включен
11	Член домена: шифрование данных безопасного канала, когда это возможно	Включен	Включен
12	Член домена: цифровая подпись данных безопасного канала, когда это возможно	Включен	Включен
13	Член домена: отключить изменение пароля учетных записей компьютера	Отключен	Отключен
14	Член домена: максимальный срок действия пароля учетных записей компьютера	30 дней	30 дней
15	Член домена: требует стойкого ключа сеанса	Включен	Включен
16	Интерактивный вход в систему: не отображать последнее имя пользователя	Включен	Включен
17	Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL	Отключен	Отключен
18	Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)	0 входов	0 входов
19	Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее	14 дней	14 дней
20	Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера	Включен	Включен
21	Интерактивный вход в систему: поведение при извлечении смарт-карты	Блокировка рабочей станции	Блокировка рабочей станции
22	Клиент сети Microsoft: использовать цифровую подпись (всегда)	Включен	Включен
23	Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	Включен	Включен
24	Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам	Отключен	Отключен

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
25	Сервер сети Microsoft: длительность простоя перед отключением сеанса	15 минут	15 минут
26	Сервер сети Microsoft: использовать цифровую подпись (всегда)	Включен	Включен
27	Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)	Включен	Включен
28	Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа	Включен	Включен
29	Автоматический вход в систему	Отключен	Отключен
30	Запрет IP маршрутизации от источника	Источник направляющий маршрутизацию полностью отключен	Источник направляющий маршрутизацию полностью отключен
31	Изменение таблицы маршрутизации в ответ на ICMP-редирект пакеты	Отключен	Отключен
32	Интервал отправки пакетов проверки активности соединения	300000 миллисекунд	300000 миллисекунд
33	Не производить показ NetBIOS имени компьютера	Включен	Включен
34	Запрет на создание коротких NetBIOS имен	Отключен	Включен
35	Использование IRDP-протокола	Отключен	Отключен
36	Количество неудачных попыток передачи данных, перед разрывом соединения	3 раз	3 раз
37	Предельный размер (в процентном соотношении) журнала событий, по достижении которого система будет формировать предупреждение	90 процентов	90 процентов
38	Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями	Включен	Включен

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
39	Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями	Включен	Включен
40	Сетевой доступ: не разрешать сохранение учетных данных или цифровых паспортов .NET для сетевой проверки подлинности пользователя	Включен	Включен
41	Сетевой доступ: разрешать применение разрешений 'Для всех' к анонимным пользователям	Отключен	Отключен
42	Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам	Включен	Включен
43	Сетевой доступ: разрешать анонимный доступ к именованным каналам	Источник доступа:Не определено	Источник доступа:COMNAP COMNODE SQL\QUERY SPOOLSS EPMAPPER LOCATOR TrkWks TrkSvr

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
44	Сетевой доступ: удаленно доступные пути и вложенные пути реестра	список: System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	список: System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
45	Сетевой доступ: удаленно доступные пути реестра	список: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	список: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion
46	Сетевой доступ: разрешать анонимный доступ к общим ресурсам	список: Не определено	список: Ни для кого(список пуст)
47	Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей	Обычная - локальные пользователи удостоверяются как они сами	Обычная - локальные пользователи удостоверяются как они сами
48	Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля	Включен	Включен
49	Сетевая безопасность: уровень проверки подлинности LAN Manager	отправлять только NTLMv2-ответ (отказывать LM)	отправлять только NTLMv2-ответ (отказывать LM и NTLM)
50	Сетевая безопасность: требование цифровой подписи для LDAP-клиента	Согласование подписывания	Согласование подписывания
51	Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)	Требовать сеансовую безопасность NTLMv2, требовать 128-разрядное шифрование	Требовать сеансовую безопасность NTLMv2, требовать 128-разрядное шифрование

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
52	Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)	Требовать сеансовую безопасность NTLMv2, требовать 128-разрядное шифрование	Требовать сеансовую безопасность NTLMv2, требовать 128-разрядное шифрование
53	Консоль восстановления: разрешить автоматический вход администратора	Отключен	Отключен
54	Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам	Включен	Отключен
55	Завершение работы: разрешить завершение работы системы без выполнения входа в систему	Отключен	Отключен
56	Завершение работы: очистка страничного файла виртуальной памяти	Отключен	Отключен
57	Системная криптография: обязательное применение сильной защиты ключей пользователей, хранящихся на компьютере	пользователь получает запрос при первом использовании ключа	пользователь должен вводить пароль при каждом использовании ключа
58	Системная криптография: использование FIPS-совместимые алгоритмы для шифрования, хэширования и подписывания	Отключен	Отключен
59	Системные объекты: учитывать регистр для подсистем, отличных от Windows	Включен	Включен
60	Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов(запретить доступ к основным базовым библиотекам)	Включен	Включен
61	Параметры системы: необязательные подсистемы	список: Ни для кого(список пуст)	список: Ни для кого(список пуст)

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «Specialized Security – Limited Functionality»
62	Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ	Отключен	Включен
63	Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов(запретить доступ к основным базовым библиотекам)	Включен	Включен

Параметр безопасности «Учетные записи: ограничить использование пустых паролей только для консольного входа» определяет, можно ли использовать локальные учетные записи с пустыми паролями не только для интерактивного входа в систему. Если активировать данный параметр, то локальные учетные записи с пустыми паролями нельзя будет использовать для связи с компьютерами по сети через сетевые службы Windows или службы терминалов. Действие этого параметра касается только локальных учетных записей и не распространяется на учетные записи домена.

В случае использования учетных записей с пустыми паролями нарушитель может ими легко воспользоваться, поскольку в этом случае ему будет достаточно определить имя учетной записи пользователя. Поэтому в обоих вариантах рассматриваемых конфигураций параметр «Учетные записи: ограничить использование пустых паролей только для консольного входа» должен иметь значение «Включен».

Параметр безопасности «Устройства: разрешать отстыковку без входа в систему» определяет, должен ли пользователь входить в систему, чтобы запросить отсоединение переносного компьютера от стыковочного узла. Если этот параметр включен, пользователь может запросить отстыковку компьютера без входа в систему. В противном случае, пользователь обязан входить в систему для того, чтобы запросить отстыковку, причем в этот момент он должен обладать разрешением «Отключение компьютера от стыковочного узла». Данное требование относится к обеим конфигурациям, поэтому параметр «Устройства: разрешать отстыковку без входа в систему» принимает значение «Отключен».

Параметр безопасности «Устройства: разрешено форматировать и извлекать съемные носители» определяет, кто имеет право форматировать и извлекать съемный носитель. Пользователь, не обладающий такой привилегией, не сможет взять носитель с одного компьютера и получить к нему доступ на другом компьютере, где у него есть права локального администратора.

Исходя из этого, данный параметр безопасности в конфигурациях «Enterprise» и «Specialized Security – Limited Functionality» должен иметь значение «Администраторы».

Параметр безопасности «Устройства: запретить пользователям установку драйверов принтера» определяет, кто имеет право устанавливать драйвер принтера, чтобы получить возможность использовать сетевой принтер. При отключении данного параметра любой пользователь получает возможность устанавливать драйвер принтера, в то время как под драйвером может скрываться злонамеренный программный код. С помощью этого параметра можно предотвратить загрузку и установку ненадежного драйвера принтера пользователями, не имеющими на это права.

Поэтому в обеих рассматриваемых конфигурациях параметр «Устройства: запретить пользователям установку драйверов принтера» должен иметь значение «Включен».

Параметр безопасности «Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям» определяет, может ли компакт-диск быть доступен одновременно локальным и удаленным пользователям. Если этот параметр активирован, дисковод компакт-дисков доступен только пользователям, выполнившим интерактивных вход в систему. В тоже время, если данный параметр активирован, но никто не выполнил локальных вход в систему, дисковод компакт-дисков может быть доступен удаленным пользователям.

По этой причине, в конфигурации безопасности «Enterprise» данный параметр может иметь значение «Не определено», а в конфигурации «Specialized Security – Limited Functionality» принимает значение «Отключен».

Параметр безопасности «Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям» определяет, может ли гибкий диск быть доступен одновременно локальным и удаленным пользователям. Если этот параметр активирован, дисковод гибких дисков доступен только пользователям, выполнившим интерактивных вход в систему. В тоже время, если данный параметр

активирован, но никто не выполнил локальных вход в систему, дисковод гибких магнитных дисков может быть доступен удаленным пользователям.

По этой причине, в конфигурации безопасности «Enterprise» данный параметр может иметь значение «Не определено», а в конфигурации «Specialized Security – Limited Functionality» принимает значение «Включен».

Параметр безопасности «Член домена: отключить изменение пароля учетных записей компьютера» определяет должен ли член домена периодически менять свой пароль учетной записи компьютера. Если этот параметр включен, член домена не будет пытаться сменить пароль учетной записи компьютера. Если параметр отключен, член домена будет пытаться сменить пароль учетной записи компьютера в соответствии с параметром «Член домена: максимальный срок действия пароля учетных записей компьютера». Компьютеры, которые не осуществляют самостоятельную автоматическую смену пароля для собственной учетной записи, подвержены риску, связанному с определением злоумышленником пароля для доменной учетной записи.

По этой причине, в конфигурациях безопасности «Enterprise» и «Specialized Security – Limited Functionality» параметр «Член домена: отключить изменение пароля учетных записей компьютера» должен иметь значение «Отключен».

Параметр безопасности «Член домена: максимальный срок действия пароля учетных записей компьютера» определяет максимальный допустимый срок службы пароля учетной записи компьютера. По умолчанию члены домена автоматически изменяют свой собственный пароль каждые 30 дней. Увеличение данного временного интервала, или установка значения параметра равным 0, что приведет к невозможности смены компьютерами собственных паролей, предоставит злоумышленнику только больше времени на организацию и осуществление атаки подбора пароля учетной записи компьютера по словарю (словарная атака типа «brute force»).

Исходя из этого, в конфигурациях безопасности «Enterprise» и «Specialized Security – Limited Functionality» максимальный срок действия пароля учетных записей компьютера должен быть равен 30 дням.

Параметр безопасности «Интерактивный вход в систему: не отображать последнее имени пользователя» определяет, будет ли в соответствующем окне входа в систему на каждом компьютере отображаться имя учетной записи последнего из пользователей, осуществившим интерактивный вход в систему. Активация данного

параметра не позволит нарушителю собирать сведения об именах учетных записей непосредственно с экранов компьютеров. Исходя из этого, в обеих рассматриваемых конфигурациях для параметра необходимо установить значение «Включен».

Параметр безопасности «Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL» определяет необходимость обеспечения контролируемого входа в систему посредством нажатия пользователем комбинации клавиш CTRL+ALT+DEL. Активация этого параметра означает, что пользователям нет необходимости использовать указанную комбинацию клавиш для входа в систему, что снижает уровень безопасности, поскольку дает нарушителю возможность войти в клиентский компьютер, не имея достаточных полномочий.

Поэтому, в обеих рассматриваемых конфигурациях для данного параметра должно быть определено значение «Отключен».

Параметр безопасности «Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)» определяет, сколько учетных данных система может хранить в кэше. Сохранение учетных данных в кэше позволяет входить в систему, если компьютер отключен от сети или контроллер домена недоступен.

Максимальный уровень безопасности достигается при значении этого параметра равном 0, однако в этом случае пользователи не смогут войти в систему, если по какой-то причине отсутствует доступ к котроллеру домена.

Исходя их этого, в конфигурациях «Enterprise» и «Specialized Security - Limited Functionality» данный параметр должен иметь значение «0».

Параметр безопасности «Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее» определяет, за какое время до окончания срока действия пароля пользователи получат предупреждение об этом. Рекомендуется предупреждать пользователей за 14 дней до окончания срока действия их паролей.

Параметр безопасности «Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера» определяет необходимость проверки контроллером домена подлинности доменной учетной записи для разблокирования компьютера. Если действие этого параметра отменено, для входа в компьютер можно воспользоваться учетными данными, сохраненными в кэше. При включении данного параметра необходимо убедиться, что все компьютеры имеют сетевой доступ к контроллеру домена. В конфигурациях «Enterprise» и «Specialized

Security – Limited Functionality» данный параметр должен иметь значение «Включен».

Параметр безопасности «Интерактивный вход в систему: поведение при извлечении смарт-карты» определяет, что происходит при извлечении смарт-карты пользователя, вошедшего в систему, из устройства чтения смарт-карт. В случае выбора при настройке данного параметра безопасности значения «Блокировка рабочей станции» клиентский компьютер при извлечении смарт-карты будет заблокирован, что позволит пользователю заблокировать собственный сеанс доступа, не завершая его. При выборе варианта «Принудительный выход из системы» при извлечении смарт-карты произойдет автоматическое завершение сеанса работы пользователя. В качестве рекомендуемого значения параметра безопасности «Интерактивный вход в систему: поведение при извлечении смарт-карты» в обеих конфигурациях следует выбрать «Блокировка рабочей станции».

Использование параметра безопасности «Клиент сети Microsoft: использовать цифровую подпись (всегда)» позволит обязать компьютер использовать цифровую подпись в клиентских сеансах.

Протокол проверки подлинности SMB (Server Message Block) поддерживает взаимную проверку подлинности, позволяющую отражать атаки «третьей стороны» (man-in-the-middle), и проверку подлинности сообщений, обеспечивающую защиту от атак через активные сообщения. Средства подписи SMB обеспечивают такую проверку, помещая в каждый пакет SMB цифровую подпись, которая затем проверяется и клиентом, и сервером.

Чтобы использовать подписи SMB, необходимо разрешить или обязать добавление подписей как на SMB-клиенте компьютере, так и на SMB-сервере. Если подписи SMB разрешены на сервере, то клиенты, на которых они также разрешены, будут использовать этот протокол для цифровой подписи пакетов во всех последующих сеансах. Если подписи SMB являются обязательными на сервере, клиент сможет установить сеанс с данным сервером только при условии включение режима подписи SMB на самом клиенте.

Активирование данного параметра безопасности должно быть осуществлено в обоих конфигурациях.

При активации параметра безопасности «Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)» SMB-клиент подписывает SMB-пакет, посылаемый SMB-серверу, на котором режим подписи пакетов либо просто разрешен, либо обязателен. Отключение этого параметра означает, что SMB-клиент не будет подписывать пакеты, посылаемые SMB-серверу, даже если для сервера эта

процедура является обязательной. Активация данного параметра для SMB-клиентов позволит им полноценно использовать подпись пакетов при взаимодействии со всеми клиентскими компьютерами и серверами сети, что усилит безопасность сетевого взаимодействия.

Исходя из этого, в обеих рассматриваемых конфигурациях для параметра необходимо установить значение «Включен».

При отключении параметра безопасности «Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам» SMB-редиректор не сможет посылать пароли в виде обычного текста SMB-серверам с другими операционными системами, которые не поддерживают шифрование паролей при проверке подлинности. В связи с тем, что активация данного параметра дает разрешение на передачу по сети незашифрованных паролей в обеих конфигурациях для него необходимо установить значение «Отключен».

Параметр безопасности «Сервер сети Microsoft: время бездействия до приостановки сеанса» определяет продолжительность временного интервала, по истечении которого произойдет приостановка SMB-сеанса. С помощью данного параметра администраторы могут задавать время простоя до приостановки SMB-сеанса. Как только клиент возобновляет свои действия, сеанс автоматически восстанавливается. В обеих рассматриваемых конфигурациях данному параметру рекомендуется присваивать значение «15 минут».

Параметр безопасности «Сервер сети Microsoft: использовать цифровую подпись (всегда)» определяет, требуется ли от SMB-сервера обязательная подпись SMB-пакетов. Активация этого параметра имеет дополнительные преимущества в комбинированной среде, поскольку не позволяет клиентам более низкого уровня использовать свою рабочую станцию в качестве сетевого сервера. Данный параметр следует активировать, если среда предприятия целиком построена на операционной системе Microsoft® Windows Server™ 2003 и службе каталогов Active Directory. Поэтому в обеих рассматриваемых конфигурациях для параметра необходимо установить значение «Включен».

Параметр безопасности «Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)» определяет, следует ли SMB-серверу подписывать SMB-пакеты. При активации данного параметра SMB-сервер ставит цифровую подпись, если того требует SMB-клиент, которому предназначен пакет. Активация данного параметра для SMB-клиентов позволит им полноценно использовать подпись пакетов при

взаимодействии со всеми клиентскими компьютерами и серверами сети. Исходя из этого, для обеих рассматриваемых конфигураций для параметра необходимо установить значение «Включен».

Параметр безопасности «Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа» определяет, следует ли отключать пользователей, работающих на локальном компьютере вне отведенных им рабочих часов. Этот параметр влияет на работу блока сообщений сервера SMB. Когда он активирован, клиентские сеансы с участием службы SMB будут принудительно прекращаться по истечении периода времени, в течение которого клиенту разрешен вход в систему. Если этот параметр отключен, начатый сеанс будет продолжен и после окончания времени, разрешенного клиенту для входа в систему. Поэтому в обеих рассматриваемых конфигурациях данный параметр должен иметь значение «Включен».

Параметр безопасности «Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями» позволяет проконтролировать, смогут ли анонимные пользователи узнать число учетных записей в базе данных диспетчера учетных записей безопасности SAM (Security Account Manager). В случае активации данного параметра пользователи с анонимным подключением не смогут перечислять имена учетных записей домена на рабочих станциях. Этот параметр вводит дополнительные ограничения на анонимные подключения. Поэтому в обеих рассматриваемых конфигурациях для данного параметра должно быть установлено значение «Включен».

Параметр безопасности «Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями» позволяет проконтролировать, смогут ли анонимные пользователи узнать число учетных записей SAM и совместно используемых ресурсов. В случае активации данного параметра анонимные пользователи не смогут перечислить имена доменных учетных записей и совместно используемые сетевые имена на рабочих станциях. Поэтому в обеих рассматриваемых конфигурациях для данного параметра должно быть установлено значение «Включен».

Параметр безопасности «Сетевой доступ: не разрешать сохранение учетных данных или цифровых паспортов .NET для сетевой проверки подлинности пользователя» определяет, можно ли хранить на локальном компьютере учетные данные и пароли для проверки подлинности. В обеих рассматриваемых конфигурациях для указанного параметра необходимо установить значение «Включен».

Параметр безопасности «Сетевой доступ: разрешить применение разрешений для всех к анонимным пользователям» определяет, какие дополнительные разрешения предоставляются при анонимном подключении к компьютеру. Microsoft® Windows Server™ 2003 предоставляет анонимным пользователям возможность выполнять ряд операций (например, производить перечисление имен учетных записей домена и сетевых ресурсов). Это удобно в случае, если администратору требуется предоставить доступ пользователям в доверенном домене, в котором не поддерживается двусторонние доверительные отношения. По умолчанию из маркера доступа, создаваемого для анонимных подключений, удаляется идентификатор безопасности группы «Все». Поэтому разрешения, предоставленные группе безопасности «Все», не применяются к анонимным пользователям. Если данный параметр установлен, анонимный пользователь получит доступ только к тем ресурсам, для которых ему явным образом предоставлено разрешение. Поскольку при включении данной политики, анонимные пользователи смогут получить перечень имен учетных записей пользователей и сетевых ресурсов, и в дальнейшем использовать полученную информацию для организации атак различных типов, в обеих конфигурациях безопасности использование данного параметра должно быть запрещено.

Параметр безопасности «Сетевой доступ: разрешать анонимный доступ к общим ресурсам» определяет, какие сетевые ресурсы доступны анонимным пользователям. В конфигурации безопасности «Specialized Security – Limited Functionality» данному параметру должно быть присвоено значение «Список пуст». Добавление иных общих ресурсов связано с потенциальной угрозой их доступности любому сетевому пользователю, что в свою очередь может привести к компрометации или утрате информации.

Параметр безопасности «Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей» определяет, как проверяется подлинность сетевых подключений, сделанных с помощью локальных учетных записей. Значение «Обычная» обеспечивает тонкую регулировку доступа к ресурсам. Задав это значение параметра, можно предоставить различным пользователям различные варианты доступа к одному и тому же ресурсу. Значение «Только гость» позволяет сделать всех пользователей равноправными. В этом случае для получения одинакового уровня доступа к данному ресурсу все пользователи проходят проверку подлинности в варианте «Только гость». Активация данного параметра не влияет на сетевые подключения, сделанные с помощью доменных учетных записей, и на интерактивные подключения.

Поэтому для данного параметра необходимо задать значение «Обычная – локальные пользователи удостоверяются как они сами», которое будет затрагивать пользователей, входящих в систему в любой из двух рассматриваемых конфигураций.

Параметр безопасности «Сетевая безопасность: не хранить хеш-значений LANManager при следующей смене пароля» определяет, будет ли хранить LAN Manager (LM) при смене пароля хеш-значение для нового пароля. Используя файл диспетчера учетных записей SAM, нарушители могут получить доступ к именам пользователей и хеш-значениям паролей. Для определения паролей злоумышленники могут воспользоваться средствами подбора паролей. Включение данного параметра безопасности не исключает возможность атак такого типа, но существенно затрудняет их выполнение. Поэтому в обеих рассматриваемых конфигурациях для параметра должно быть установлено значение «Включен».

Параметр безопасности «Сервер сети Microsoft: отключать клиентов по истечении допустимых часов работы» определяет необходимость принудительного завершения сеанса работы с SMB-сервером для клиентов, у которых закончилось время, разрешенное для входа в систему. Это позволяет предотвратить несанкционированное использование рабочих станций в неположенное время. В обеих рассматриваемых конфигурациях данный параметр должен иметь значение «Включен».

Параметр безопасности «Сетевая безопасность: уровень проверки подлинности LAN Manager» определяет метод проверки подлинности запросов и ответов при сетевых подключениях к клиентским компьютерам с системами, отличными от операционных систем семейства Microsoft® Windows® 2000 и Microsoft® Windows Server™ 2003. Метод проверки подлинности LM наименее безопасен, он позволяет легко обнаружить в сети зашифрованные пароли и взломать их. Несколько более безопасным является метод NTLM (NT LanManager). Метод NTLMv2 представляет собой более надежную версию метода NTLM, имеющуюся в системах Microsoft® Windows Server™ 2003, Microsoft® Windows® 2000 и Windows® NT 4.0 с пакетами обновления, начиная с SP4. Метод NTLMv2 также доступен в системах Windows 95/98 при использовании службы Directory Services Client. Данный параметр для конфигурации «Enterprise» должен соответствовать значению «Запрет контроллеру домена использовать аутентификацию LM т.е отправлять только NTLMv2-ответ. Отказывать LM», а для конфигурации «Specialized Security – Limited

Functionality» - значению «Необходимость применять при аутентификации только протокол NTLMv2 т.е отправлять только NTLMv2-ответ. Отказывать LM & NTLM ».

Параметр безопасности «Сетевая безопасность: требование цифровой подписи для LDAP клиента» определяет уровень подписывания данных, требуемый от клиента, посылающего LDAP-запрос серверу. Поскольку неподписанный сетевой трафик подвержен атакам «третьей стороны» (man-in-the-middle), то злоумышленник сможет вынудить LDAP-сервера принять решение, базируясь на ложном запросе от LDAP-клиента. Таким образом, в конфигурациях «Enterprise» и «Specialized Security – Limited Functionality» данный параметр безопасности должен принимать значение «Согласование подписывания».

Параметр безопасности «Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)» определяет минимальные стандарты безопасности для сеансов связи между приложениями для клиента. Microsoft® Windows Server™ 2003 поддерживает два варианта проверки подлинности по схеме «запрос/ответ» при входе в сеть: LAN Manager и NTLM версии 2. Протокол LAN Manager обеспечивает совместимость с уже действующими платформами клиентов и серверов. Протокол NTLM обеспечивает повышенный уровень безопасности для подключений между клиентами и серверами. Для обеспечения сеансовой безопасности для клиентов данный параметр в обеих конфигурациях безопасности должен принимать следующие значения:

– требовать 128-разрядное шифрование;
– требовать сеансовую безопасность NTLMv2.

Параметр безопасности «Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)» определяет минимальные стандарты безопасности для сеансов связи между приложениями на сервере. Для обеспечения сеансовой безопасности для серверов данный параметр в обеих конфигурациях безопасности должен принимать следующее значения:

– требовать 128-разрядное шифрование;
– требовать сеансовую безопасность NTLMv2.

Параметр безопасности «Консоль восстановления: разрешить автоматический вход администратора» определяет, следует ли вводить пароль учетной записи администратора, прежде чем будет предоставлено право доступа к системе. Включение этого параметра разрешает автоматический вход в систему без необходимости

ввода пароля на консоли восстановления, что представляет угрозу безопасности, поскольку любой человек в режиме консоли восстановления сможет получить неограниченный доступ к локальным ресурсам. Поэтому в обеих рассматриваемых конфигурациях данный параметр должно быть отключен.

При активации параметра безопасности «Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам» пользователи получают полный доступ ко всему дисковому пространству системы. Кроме того, они могут копировать файлы с жесткого диска на гибкий диск. При отключении данного параметра действует запрет на копирование файлов с жесткого диска на гибкий диск, а также ограничивается доступ к дискам и каталогам. В конфигурации «Enterprise» данный параметр может принимать значение «Включен». В свою очередь, в конфигурации «Specialized Security – Limited Functionality» данный параметр должен иметь значение «Отключен».

Параметр безопасности «Завершение работы: разрешить завершение работы системы без выполнения входа в систему» определяет, нужно ли пользователю входить в систему, чтобы завершить ее работу. При активации данного параметра команда на завершение работы операционной системы становится доступной в окне входа в систему Windows, что позволяет пользователям, имеющим локальный доступ к консоли завершать работу системы или её перезагрузку без выполнения процедур входа в нее. В конфигурациях «Enterprise» и «Specialized Security – Limited Functionality» данный параметр должен иметь значение «Отключен».

Параметр безопасности «Завершение работы: очистка страничного файла виртуальной памяти» определяет, должна ли при завершении работы системы выполняться очистка страничного файла виртуальной памяти, который во время работы операционной системы используется виртуальной памятью для записи неиспользуемых страниц памяти на диск. При включении данного параметра сведения, которые могли попасть в страничный файл, окажутся недоступными несанкционированным пользователям, получившим к нему прямой доступ после завершения работы системы. Поэтому в конфигурациях «Enterprise» и «Specialized Security – Limited Functionality» данный параметр может быть отключен.

Параметр безопасности «Системные объекты: учитывать регистр для подсистем, отличных от Windows» определяет, распространяется ли требование независимости от регистра символов на все подсистемы операционной системы. Подсистема

Microsoft Win32® не требует учитывать регистр символов. Однако в других подсистемах, таких как POSIX, ядро поддерживает различение регистров символов. Если данный параметр включен, то все объекты каталога, символические ссылки и объекты ввода-вывода, включая файлы, используются без учета регистра символов. При отключении этого параметра подсистема Microsoft Win32® не сможет перейти в режим учета регистра символов. Для обеспечения согласованности имен объектов каталога, символических ссылок и объектов ввода-вывода, в конфигурациях «Enterprise» и «Specialized Security – Limited Functionality» данный параметр безопасности должен быть включен.

Параметр безопасности «Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок)» определяет уровень строгости стандартной дискреционной таблицы управления доступом DACL (Discretional Access Control List) для объектов. Служба Active Directory ведет глобальный список общих системных ресурсов, таких как имена устройств DOS, мьютексы и семафоры. Благодаря этому можно отыскивать нужные объекты и предоставлять их в общий доступ различным процессам. При создании объекта создается стандартная таблица управления доступом DACL, соответствующая данному типу объектов. В ней указано, кто имеет доступ к объекту, и какие разрешения доступа предоставлены.
Если данная политика включена, стандартная таблица DACL становится более строгой: пользователям, не являющимся администраторами, разрешается читать содержимое общих объектов, но запрещается изменять общие объекты, созданные другими пользователями. Следовательно в обеих конфигурациях безопасности данная политика должна быть включена.

Параметры безопасности журналов регистрации событий

В журналы регистрации событий заносятся все подлежащие аудиту события. В разделе «Журнал событий» объекта групповой политики определяются атрибуты, относящиеся к журналам «Приложение», «Безопасность» и «Система», к которым относятся максимальный размер журнала, права доступа к журналам и настройки и способы их хранения.

Параметры журналов регистрации событий следует настраивать с помощью редактора групповой политики в следующем разделе пространства имен объекта групповой политики: Конфигурация компьютера\Конфигурация Windows\Параметры безопасности \Журнал событий (см. таблицу А.2.6).

Таблица А.2.6 – Параметры безопасности журналов регистрации событий для компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003

Название параметра	Конфигурации безопасности	
	«Enterprise Client»	«Specialized Security – Limited Functionality»
Максимальный размер журнала приложений	16384 Кб	16384 Кб
Максимальный размер журнала безопасности	81920 Кб	81920 Кб
Максимальный размер системного журнала	16384 Кб	16384 Кб
Запретить доступ локальной группы гостей к журналу приложений	Включен	Включен
Запретить доступ локальной группы гостей к журналу безопасности	Включен	Включен
Запретить доступ локальной группы гостей к системному журналу	Включен	Включен
Сохранение событий в журнале приложений	Не определено	Не определено
Сохранение событий в журнале безопасности	Не определено	Не определено
Сохранение событий в системном журнале	Не определено	Не определено
Сохранение событий в журнале приложений	Затирать старые события по необходимости	Затирать старые события по необходимости
Сохранение событий в журнале безопасности	Затирать старые события по необходимости	Затирать старые события по необходимости
Сохранение событий в системном журнале	Затирать старые события по необходимости	Затирать старые события по необходимости

Параметр «Максимальный размер журнала приложений» определяет объем информации, которую можно сохранить в журнале приложений. Если заданный с помощью данного параметра размер слишком мал, журнал регистрации событий будет быстро переполняться и администраторам придется чаще очищать его и архивировать записи. Если размер журнала приложений будет слишком большим, это может послужить причиной высокой дефрагментации диска и, как следствие, приведет к понижению производительности системы. Значение данного параметра может варьироваться в диапазоне от 64 до 4194240 Кб. Рекомендуется задавать такое значение данного параметра, при котором будет достаточно места для записи событий, связанных с функционирование приложений, но при этом не занимать слишком много дискового пространства. Поэтому в обеих рассматриваемых конфигурациях для данного параметра рекомендуется значение 16384 Кб.

Параметр «Максимальный размер журнала безопасности» определяет объем информации, которую можно сохранить в журнале безопасности. Необходимо контролировать число событий, записываемых в журналы, и подбирать размер журнала безопасности в соответствии с существующими потребностями. Чтобы задействовать дополнительные параметры аудита, рекомендованные в данном руководстве, в во всех рассматриваемых конфигурации задаваемый по умолчанию размер журнала безопасности должен быть увеличен. Поэтому рекомендуемое значение параметра составляет 81920 Кб.

Параметр «Максимальный размер системного журнала» определяет объем информации, которую можно сохранить в журнале системных событий. Его размер должен быть установлен исходя из тех же критериев, что и в случае с журналом приложений.

Параметры «Запретить доступ локальной группы гостей к журналу приложений», «Запретить доступ локальной группы гостей к журналу безопасности» и «Запретить доступ локальной группы гостей к системному журналу» определяют, имеют ли анонимные пользователи право доступа к журналам приложений, безопасности и системных событий. Поскольку нарушитель, успешно вошедший в систему с правами гостя, может получить важные сведения о ней, просмотрев журналы событий (гости по умолчанию имеют доступ к ряду журналов регистрации событий), и использовать в дальнейшем полученные сведения для организации атак, поэтому данные параметры во всех конфигурациях безопасности должны быть активированы. Запрет на просмотр всех журналов регистрации событий для пользователей, не прошедших проверку, является рекомендуемым решением с точки зрения безопасности.

Параметры «Сохранение событий в журнале приложений», «Сохранение событий в журнале безопасности» и «Сохранение событий в системном журнале» определяют, сколько дней должны сохраняться имеющие важность события в соответствующих журналах регистрации событий, до того, как они будут затерты следующими записями. Данные значения нужно указывать, только если выполняется архивация журнала через запланированные интервалы времени и если проверено, что максимальный размер журнала достаточно велик. Указанный параметр действует одновременно с параметром, определяющим способ сохранения событий в соответствующем журнале. Если для способа сохранения журнала выбран вариант «Затирать старые события по необходимости», соответствующий параметр «Сохранение событий в журнале…» автоматически примет значение «Не определено».

Поэтому во всех рассматриваемых конфигурациях безопасности для параметров «Сохранение событий в журнале приложений», «Сохранение событий в журнале безопасности» и «Сохранение событий в системном журнале» необходимо задавать значение «Не определено», так как для соответствующих параметров, определяющих способ сохранения событий, выбран вариант «Затирать старые события по мере необходимости».

Параметры «Сохранение событий в журнале приложений», «Сохранение событий в журнале безопасности» и «Сохранение событий в системном журнале» определяют, как операционная система будет обрабатывать соответствующие категории событий, когда журналы регистрации событий достигнут своего максимального размера, т.е. определяет способ пополнения журналов приложений, безопасности и системных событий. С целью снижения издержек администрирования и, исходя из установленных размеров журналов регистрации событий, рекомендуемым значением в рассматриваемых конфигурациях для всех трех типов журналов является «Затирать старые события по мере необходимости».

Группы с ограниченным доступом

Параметр «Группы с ограниченным доступом» позволяет регулировать принадлежность групп безопасности в операционной системе Microsoft® Windows Server™ 2003. При вводе ограничений доступа для групп безопасности следует исходить из существующих потребностей. В данном руководстве к группам с ограниченным доступом

следует относить группы безопасности, которым делегированы полномочия по управлению ОП, содержащих учетные записи компьютеров, выполняющих сходные роли, и применяемым к ним объектам групповой политики. Если в структуре организации задействован механизм делегирования полномочий, необходимо тщательно контролировать состав групп безопасности, которым данных предоставляются административные полномочия.

Членство в группах с ограниченным доступом следует настраивать в операционной системе Microsoft® Windows Server™ 2003 в редакторе групповой политики в следующем разделе пространства имен объекта групповой политики: `Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Группы с ограниченным доступом`.

Администраторы могут задавать группы с ограниченным доступом через объекты групповой политики, добавляя нужную группу прямо в раздел «Группы с ограниченным доступом» пространства имен объектов групповой политики. Когда группа определена в качестве группы с ограниченным доступом, для нее можно назначать членов, а также задавать другие группы, куда она сама входит в качестве члена. Если для группы не определено ни одного члена, доступ в нее будет полностью ограничен.

Рекомендуется также вводить ограничения для всех встроенных групп, которые не планируется использовать на предприятии.

Системные службы

При установке операционной системы Microsoft® Windows Server™ 2003 создаются и настраиваются стандартные системные службы, которые начинают функционировать при запуске системы. Однако при функционировании в том или ином окружении для нормальной работы системы ряд служб не требуется. Любая служба или приложение является потенциальным объектом атаки. Поэтому ненужные службы или исполняемые файлы следует отключить или удалить.

Параметры системных служб операционной системы Microsoft® Windows Server™ 2003 следует настраивать в редакторе групповой политики в следующем разделе пространства имен объекта групповой политики: `Конфигурация компьютера\ Конфигурация Windows\Параметры безопасности\Системные службы`.

Рекомендуемые параметры настройки системных служб операционной системы Microsoft® Windows Server™ 2003 представлены в таблице А.2.7.

Таблица А.2.7 – Параметры настройки системных служб для компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003

Системная служба	Имя службы	Режим запуска службы в конфигурации	
		«Enterprise Client»	«Specialized Security – Limited Functionality»
Оповещатель	Alerter	Запрещен	Запрещен
Служба шлюза уровня приложения	ALG	Запрещен	Запрещен
Управление приложениями	AppMgmt	Запрещен	Запрещен
Служба состояния сеанса ASP .NET	aspnet_state	Запрещен	Запрещен
Автоматическое обновление	wuauserv	Запрещен	Запрещен
Фоновая интеллектуальная служба передачи	BITS	Вручную	Вручную
MS Software Shadow Copy Provider	SwPrv	Вручную	Вручную
Сервер папки обмена	ClipSrv	Запрещен	Запрещен
Система событий COM+	EventSystem	Вручную	Вручную
Системное приложение COM+	COMSysApp	Запрещен	Запрещен
Обозреватель компьютеров	Browser	Автоматически	Автоматически
Службы криптографии	CryptSvc	Автоматически	Автоматически
DHCP-клиент	Dhcp	Автоматически	Автоматически
Распределенная файловая система	Dfs	Запрещен	Запрещен
Клиент отслеживания изменившихся связей	TrkWks	Запрещен	Запрещен
Сервер отслеживания изменившихся связей	TrkSvr	Запрещен	Запрещен

Системная служба	Имя службы	Режим запуска службы в конфигурации	
		«Enterprise Client»	«Specialized Security – Limited Functionality»
Координатор распред-еленных транзакций	MSDTC	Запрещен	Запрещен
DNS-клиент	Dnscache	Автоматически	Автоматически
Служба регистрации ошибок	ERSvc	Запрещен	Запрещен
Журнал событий	Eventlog	Автоматически	Автоматически
Служба факсов	Fax	Запрещен	Запрещен
Служба репликации файлов	NtFrs	Запрещен	Запрещен
Служба FTP-публикации	MSFtpsvr	Запрещен	Запрещен
Справка и поддержка	helpsvc	Запрещен	Запрещен
HTTP SSL	HTTPFilter	Запрещен	Запрещен
Доступ к HID-устройствам	HidServ	Запрещен	Запрещен
Служба IIS Admin	IISADMIN	Запрещен	Запрещен
Служба веб-публикации	W3SVC	Запрещен	Запрещен
Служба COM записи компакт-дисков IMAPI	ImapiService	Запрещен	Запрещен
Служба индексирования	Cisvc	Запрещен	Запрещен
Брандмауэр Интернета (ICF) /Общий доступ к Интернету (ICS)	SharedAccess	Запрещен	Запрещен
Intersite Messaging	IsmServ	Запрещен	Запрещен
Службы IPSEC	PolicyAgent	Автоматически	Автоматически
Центр распространения ключей Kerberos	Kdc	Запрещен	Запрещен
Служба учета лицензий	LicenseService	Запрещен	Запрещен
Диспетчер логических дисков	dmserver	Вручную	Вручную
Служба администрирова-	dmadmin	Вручную	Вручную

Системная служба	Имя службы	Режим запуска службы в конфигурации	
		«Enterprise Client»	«Specialized Security – Limited Functionality»
ния диспетчера логических дисков			
Служба сообщений	Messenger	Запрещен	Запрещен
Служба сетевого входа в систему (Netlogon)	Netlogon	Автоматически	Автоматически
NetMeeting Remote Desktop Sharing	mnmsrvc	Запрещен	Запрещен
Сетевые подключения	Netman	Вручную	Вручную
Служба сетевого DDE	NetDDE	Запрещен	Запрещен
Диспетчер сетевого DDE	NetDDEdsdm	Запрещен	Запрещен
Служба сетевого расположения	NLA	Вручную	Вручную
Поставщик поддержки безопасности NTLM	NtLmSsp	Автоматически	Автоматически
Журналы и оповещения производительности	SysmonLog	Вручную	Вручную
Plug and Play	PlugPlay	Автоматически	Автоматически
Служба серийных номеров переносных устройств мультимедиа	WmdmPmSN	Запрещен	Запрещен
Диспетчер очереди печати	Spooler	Запрещен	Запрещен
Защищенное хранилище	Protected-Storage	Автоматически	Автоматически
Диспетчер автоматических подключений удаленного доступа	RasAuto	Запрещен	Запрещен
Диспетчер подключений удаленного доступа	RasMan	Запрещен	Запрещен

Системная служба	Имя службы	Режим запуска службы в конфигурации	
		«Enterprise Client»	«Specialized Security – Limited Functionality»
Диспетчер сеанса справки для удаленного рабочего стола	RDSessMgr	Запрещен	Запрещен
Удаленный вызов процедур (RPC)	RpcSs	Автоматически	Автоматически
Локатор удаленного вызова процедур (RPC)	RpcLocator	Запрещен	Запрещен
Удаленный реестр	Remote-Registry	Автоматически	Автоматически
Съемные ЗУ	NtmsSvc	Вручную	Вручную
Поставщик результирующей политики	RSoPProv	Запрещен	Запрещен
Маршрутизация и удаленный доступ	RemoteAccess	Запрещен	Запрещен
Вторичный вход в систему	seclogon	Запрещен	Запрещен
Диспетчер учетных записей безопасности	SamSs	Автоматически	Автоматически
Сервер	lanmanserver	Автоматически	Автоматически
Определение оборудования оболочки	ShellHW-Detection	Запрещен	Запрещен
Смарт-карты	SCardSvr	Запрещен	Запрещен
Модуль поддержки специальной консоли администрирования	Sacsvr	Запрещен	Запрещен
Уведомление о системных событиях	SENS	Автоматически	Автоматически
Планировщик заданий	Schedule	Запрещен	Запрещен
Модуль поддержки	LMHosts	Автоматически	Автоматически

Системная служба	Имя службы	Режим запуска службы в конфигурации	
		«Enterprise Client»	«Specialized Security – Limited Functionality»
NetBIOS через TCP/IP			
Телефония	TapiSrv	Запрещен	Запрещен
Служба Telnet	TlntSvr	Запрещен	Запрещен
Службы терминалов	TermService	Автоматически	Автоматически
Лицензирование служб терминалов	TermServ-Licensing	Запрещен	Запрещен
Каталог сеанса служб терминалов	Tssdis	Запрещен	Запрещен
Темы	Themes	Запрещен	Запрещен
Источник бесперебойного питания	UPS	Запрещен	Запрещен
Диспетчер отгрузки	Uploadmgr	Запрещен	Запрещен
Служба виртуальных дисков	VDS	Запрещен	Запрещен
Теневое копирование тома	VSS	Вручную	Вручную
Веб-клиент	WebClient	Запрещен	Запрещен
Windows Audio	AudioSrv	Запрещен	Запрещен
Windows Installer	MSIServer	Автоматически	Автоматически
Инструментарий управления Windows	Wmi	Вручную	Вручную
Служба времени Windows	W32Time	Автоматически	Автоматически
Служба авто-обнаружения веб-прокси WinHTTP	WinHttpAuto-ProxySvc	Запрещен	Запрещен
Беспроводная настройка	WZCSVC	Запрещен	Запрещен
Адаптер производительности WMI	WmiApSrv	Вручную	Вручную
Рабочая станция	Lanmanwork-	Автоматически	Автоматически

Системная служба	Имя службы	Режим запуска службы в конфигурации	
		«Enterprise Client»	«Specialized Security – Limited Functionality»
	station		
Служба веб-публикаций	W3SVC	Запрещен	Запрещен

Служба «Оповещатель» посылает выбранным пользователям и компьютерам административные оповещения. Отключение этой службы приводит к прекращению получения административных оповещений программами, в которых они используются. С целью обеспечения более высокого уровня безопасности для службы «Оповещатель» во всех рассматриваемых конфигурациях должен быть установлен режим запуска «Запрещен», который препятствует запуску данной службы и соответственно передаче данных по сети.

«Служба шлюза уровня приложения» является компонентом службы общего доступа к подключению Интернета (ICS)/брандмауэра подключения к Интернету (ICF) и предназначена для поддержки подключаемых модулей, которые позволяют сетевым протоколам проходить через брандмауэр и функционировать в случае использования общего доступа к подключению Интернета. Модули шлюза уровня приложения (Application Layer Gateway) могут открывать порты и изменять данные (например, порты и IP-адреса) в составе сетевых пакетов. С целью обеспечения более высокого уровня безопасности и предотвращения возможности неуполномоченным компьютерам выступать в качестве шлюза Интернета во всех рассматриваемых конфигурациях данная служба должны быть запрещена.

Служба «Управление приложениями» обеспечивает различные сервисы установки программного обеспечения, такие, как назначение, публикация и удаление программ. Данная служба необходима для выполнения операций инсталляций и удаления программ на клиентских компьютерах, установленных в вычислительной сети, а также получения списка уже установленных программ. Поскольку во многих случаях для централизованной доставки и установки прикладных программ на серверах используется специализированное программное обеспечение, во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить.

«Служба состояния сеанса ASP .NET» предназначена для поддержки внепроцессных состояний сеанса ASP.NET. Служба хранит данные сеанса вне процесса и

использует сокеты для взаимодействия с запущенной на сервере средой ASP.NET. Во всех рассматриваемых конфигурациях безопасности указанную службу рекомендуется отключить.

Служба «Автоматическое обновление» обеспечивает автоматическую загрузку и установку обновлений для операционной системы. Для обеспечения большего контроля над процессом установки критических обновлений и выполнения загрузки только сертифицированных обновлений безопасности во всех рассматриваемых конфигурациях безопасности данная служба должна быть запрещена.

«Фоновая интеллектуальная служба передачи» выполняет передачу данных в фоновом режиме, используя резервы сети по пропускной способности. Применение службы BITS позволяет улучшить скорость и устойчивость процесса передачи файлов, а также снизить загрузку сетевого подключения. В случае если эта служба остановлена, компоненты операционной системы Windows Update, «Автоматическое обновление» и MSN Explorer не смогут автоматически загружать программы и другие сведения. Чтобы исключить поддержку возможности автоматической загрузки программ во всех рассматриваемых конфигурациях безопасности запуск указанной службы должен осуществляться вручную.

Служба «MS Software Shadow Copy Provider» обеспечивает управление теневыми копиями, полученными с использование технологии теневого копирования тома. Использование возможности теневого копирования тома позволяет системе создавать копии (контрольных точек состояния) дисковых томов, которые используются для архивации и восстановления. В случае запрета данной службы, управление теневыми копиями дисковых томов будет невозможно. По этому во всех рассматриваемых конфигурациях безопасности запуск указанной службы должен осуществляться вручную.

Служба «Сервер папки обмена» позволяет создавать и совместно использовать «страницы» данных в папке обмена, которые можно просматривать с удаленных компьютеров. Эта служба зависит от службы сетевого DDE (NetDDE) в процессе создания общих файловых ресурсов, к которым могут подключаться другие компьютеры. Чтобы обеспечить более высокий уровень безопасности для рассматриваемых конфигураций режим запуска для данной службы должен соответствовать значению «Запрещен».

«Система событий COM+» реализует поддержку службы уведомления о системных событиях (SENS), обеспечивающей автоматическое распространение событий подписавшимся компонентам COM. Данная системная служба не требуется в повседневном

режиме функционирования операционной системы, поэтому во всех рассматриваемых конфигурация безопасности она должна быть отключена.

Служба «Системное приложение COM+» обеспечивает управление настройкой и отслеживанием компонентов COM+. Поскольку данная системная служба не требуется в повседневном режиме функционирования операционной системы, поэтому во всех рассматриваемых конфигурация безопасности она должна быть отключена.

Служба «Обозреватель компьютеров» обслуживает список компьютеров в сети и выдает его программам по запросу. Если данная служба остановлена, список не будет создан или обновлен. Кроме того, служба «Обозреватель компьютеров» используется компьютерами под управлением операционных систем семейства Microsoft Windows, которым необходимо просматривать сетевые ресурсы. Компьютеры, определенные в качестве обозревателей, поддерживают список, содержащий перечень всех совместно используемых ресурсов, доступных в сети. С целью обеспечения требуемого режима функционирования вычислительной сети режим запуска службы «Обозреватель компьютеров» в рассматриваемых конфигурациях должен быть автоматическим.

«Службы криптографии» обеспечивают три службы управления ключами:

- службу баз данных каталога, которая проверяет цифровые подписи файлов Windows;
- службу защищенного корня, которая добавляет и удаляет сертификаты доверенного корневого центра сертификации с компьютера;
- службу ключей, которая позволяет подавать заявки на сертификаты с компьютера.

Если данная служба остановлена, все эти службы управления не будут работать. Таким образом, с целью обеспечения более высокого уровня безопасности запуск «Служб криптографии» должен осуществляться автоматически.

Служба «DHCP-клиент» управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен. Данная служба обеспечивает автоматическое получение клиентом IP-адреса и всех сетевых настроек компьютера независимо от того, к какой вычислительной сети осуществлено подключение. В случае если данная служба остановлена, конфигурирование сетевых настроек должно осуществляться администратором вручную. Для всех рассматриваемых конфигураций безопасности для данной службы рекомендуется установить автоматический режим запуска. Однако, если в сети организации для адресации компьютеров используются статически выделяемые IP-адреса, службу «DHCP-клиент» рекомендуется отключить.

Служба «Распределенная файловая система DFS» объединяет разрозненные общие файловые ресурсы в единое логическое пространство имен и управляет данными логическими томами. В функционировании службы «Распределенная файловая система DFS» на рядовых серверах домена нет необходимости, поэтому для указанных серверов во всех режимах функционирования она должна быть запрещена. Однако, для корректного функционирования контроллеров домена для указанной службы должен быть установлен автоматический режим запуска.

Служба «Клиент отслеживания изменившихся связей» позволяет программам отслеживать перемещения связных файлов в пределах одного тома NTFS, или их перемещения на другой том NTFS того же компьютера или на другой том NTFS другого компьютера в домене. С целью обеспечения более высокого уровня безопасности служба «Клиент отслеживания изменившихся связей» во всех рассматриваемых конфигурациях должна быть запрещена.

Служба «Сервер отслеживания изменившихся связей» поддерживает клиентскую службу отслеживания распределенных связей домена для реализации надежной и эффективной поддержки связей в домене, а также обеспечивает хранение необходимой информации, которая позволяет отслеживать перемещение файлов для каждого тома в домене. В функционировании службы «Сервер отслеживания изменившихся связей» на рядовых серверах домена нет необходимости, поэтому для указанных серверов во всех режимах функционирования она должна быть запрещена. Однако, для корректного функционирования контроллеров домена для указанной службы должен быть установлен автоматический режим запуска.

Системная служба «Координатора распределенных транзакций» отвечает за координацию транзакций, распределенных в нескольких системах и диспетчерах ресурсов, например базах данных, очередях сообщений, файловых системах и других диспетчерах ресурсов с защитой транзакций. Служба DTC используется, если компоненты транзакций настраиваются через COM+, а также очередями сообщений (MSMQ) и в операциях SQL Server, которые охватывают несколько систем. Поскольку данная служба не требуется в повседневном режиме функционирования, во всех рассматриваемых конфигурациях безопасности ее рекомендуется отключить.

Служба «DNS-клиент» предназначена для разрешения DNS-имен путем запроса DNS-сервера и кэширования полученных ответов. Служба «DNS-клиент» должна быть запущена на каждом компьютере, который выполняет разрешение имен при доступе к сетевым ресурсам (в том числе к компьютерам и сетевым устройствам), и является

необходимой для обнаружения размещения контроллера домена в доменах Active Directory. Исходя из этого, режим запуска указанной службы во всех рассматриваемых конфигурациях безопасности должен быть автоматический.

«Служба регистрации ошибок» позволяет регистрировать и хранить информацию о сбоях служб и приложений, выполняющихся в нестандартной среде. Данная служба предоставляет группе поддержки продуктов Microsoft необходимую и достаточную информацию, необходимую для отладки драйверов и обработки возникающих ошибок. Если на компьютере включено уведомление об ошибках, пользователь будет уведомлен о произошедшей ошибке, однако не сможет отправить отчет об ошибках. По этим причинам, во всех рассматриваемых конфигурациях безопасности запуск указанной службы должен быть запрещен.

Служба «Журнал событий» обеспечивает поддержку сообщений журналов событий, выдаваемых Windows-программами и компонентами системы, и просмотр этих сообщений. Если указанная служба будет запрещена, администратор не сможет диагностировать возникающие в системе ошибки и отслеживать события аудита. По этому во всех рассматриваемых режимах функционирования запуск службы «Журнал событий» должен осуществляться автоматически.

«Служба факсов» совместимая с Telephony API (TAPI), обеспечивает для компьютеров возможность работы с факсами. Служба факсов позволяет пользователям отправлять и получать факсимильные сообщения из своих настольных приложений с помощью локального или общего сетевого устройства факсимильной связи. В рассматриваемых конфигурации безопасности с целью обеспечения требуемого уровня безопасности данная служба должна быть запрещена.

«Служба репликации файлов» (File Replication Service, FRS) автоматически копирует обновления файлов и папок между компьютерами, участвующими в одном наборе репликации FRS. Служба репликации файлов является стандартным модулем репликации, задачей которого является репликация общей папки SYSVOL между контроллерами домена под управлением операционной системой Microsoft® Windows Server™ 2003 в составе одного домена. Кроме того, данная служба может быть настроена на выполнение репликации файлов и папок между целевыми объектами корня распределенной файловой системы DFS. Если служба репликации файлов запрещена, репликация файлов не происходит и синхронизация данных не осуществляется. В случае с контроллером домена это может привести к проблемам функционирования. В тоже время, в функционировании указанной

службы на рядовых серверах нет необходимости. Поэтому во всех рассматриваемых конфигурациях безопасности запуск службы репликации файлов должен быть запрещен.

«Служба FTP-публикаций» обеспечивает подключение и администрирование FTP-узла с помощью оснастки IIS (Internet Information Service). Не рекомендуется устанавливать службу FTP-публикации на компьютерах под управлением операционной системы Microsoft® Windows Server™ 2003, если в ней нет непосредственной необходимости. По этой причине во всех конфигурациях безопасности, рассматриваемых в данном руководстве, службу FTP-публикаций необходимо отключить.

Служба «Справка и поддержка» обеспечивает возможность работы центра справки и поддержки на целевом компьютере. Если данная служба остановлена «Центр справки и поддержки» работать не будет. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить.

Системная служба «HTTP SSL» позволяет службам IIS выполнять функции протокола SSL (Secure Socket Layer - это открытый стандарт, который служит для установки каналов обмена зашифрованными данными с целью предотвращения перехвата конфиденциальной информации), т.е. обеспечивает безопасный протокол передачи данных гипертекста для служб HTTP, используя протокол SSL. Несмотря на то, что служба предназначена для применения с другими службами Интернета, в основном она используется для проведения электронных транзакций в Интернете в зашифрованном виде. Во всех рассматриваемых конфигурациях безопасности данную системную службу рекомендуется отключить.

«Служба веб-публикации» обеспечивает связь и администрирование веб-узла с помощью диспетчера служб IIS. Данную службу не рекомендуется устанавливать, если нет непосредственной необходимости в ее использовании. Поэтому во всех рассматриваемых конфигурациях безопасности для рядовых серверов данную системную службу рекомендуется отключить.

Служба «Доступ к HID-устройствам» обеспечивает универсальный доступ к HID-устройствам (Human Interface Devices), который активизирует и поддерживает использование заранее определенных клавиш быстрого вызова на клавиатуре, устройствах управления или иных устройствах мультимедиа. Поскольку указанная возможность в рассматриваемых конфигурациях безопасности не используется, данную службы необходимо отключить.

«Служба IIS Admin» предоставляет возможность администрирования компонентов IIS, таких как FTP-узлы, пулы приложений, веб-узлы и расширения веб-служб. Отключение

этой службы не позволяет пользователям создавать веб- и FTP-узлы на своих компьютерах. Для большинства компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003, настроенных в соответствии с одной из рассматриваемых конфигураций безопасности, эти возможности не требуются. По этим причинам во всех конфигурациях «Служба IIS Admin» должна быть отключена.

«Служба COM записи компакт-дисков IMAPI» управляет записью компакт-дисков с помощью IMAPI-интерфейса (Image Mastering Applications Programming Interface). Если данная служба остановлена, то целевой компьютер не сможет записывать компакт-диски. Поскольку для компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003, настроенных в соответствии с одной из рассматриваемых конфигураций безопасности, данная возможность не требуются, службу COM записи компакт-дисков IMAPI рекомендуется отключить.

«Служба индексирования» индексирует содержимое и свойства файлов на локальном и удаленных компьютерах, обеспечивает быстрый доступ к файлам с помощью языка запросов. Служба индексирования также обеспечивает быстрый поиск документов на локальном и удаленных компьютерах. Поскольку на компьютерах под управлением операционной системы Microsoft® Windows Server™ 2003, настроенной в соответствии с одной из рассматриваемых конфигураций безопасности, данная возможности не используется, ее рекомендуется отключить.

Служба «Брандмауэр Интернета (ICF)/Общий доступ к Интернету (ICS)» обеспечивает поддержку служб трансляции адресов, адресации и разрешения имен, а также служб предотвращения вторжения для компьютеров вычислительной сети. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

«Служба Intersite Messaging» обеспечивает обмен сообщениями между компьютерами под управлением операционной системы Microsoft® Windows Server™ 2003 с расчетом маршрута между сайтами. Данная служба необходима для поддержки межсайтовой репликации с использованием электронных сообщений (служба каталогов Active Directory поддерживает возможность репликации изменений между сайтами с использованием SMTP- или IP-транспорта). Поскольку в данной службе на рядовых серверах под управлением Microsoft® Windows Server™ 2003 нет необходимости, она должна быть отключена.

«Службы IPSec» обеспечивают безопасность сетевых подключений между сервером и клиентом в сетях TCP/IP, а также управляют политикой IP-безопасности, запускают процесс согласования ключей ISAKMP/Oakley (IKE) и согласуют настройки

политики IPSec. Во всех рассматриваемых конфигурациях безопасности для обеспечения возможности использования протокола IPSec режим запуска данных служб должен быть автоматический.

Служба «Центр распространение ключей Kerberos» функционирует только на контроллерах домена и обеспечивает регистрацию пользователей в вычислительной сети по протоколу Kerberos. Таким образом, во всех рассматриваемых конфигурациях безопасности автоматический режим запуска службы «Центр распределения ключей Kerberos» должен быть определен только для котроллеров домена.

«Служба учета лицензий» обеспечивает лицензирование клиентского доступа для компонентов операционной системы (IIS-сервер, службу терминалов), а также для продуктов, не входящих в состав операционной системы (Microsoft SQL Server, Microsoft Exchange Server). Во всех рассматриваемых конфигурациях безопасности службу учета лицензий рекомендуется запретить.

Служба «Диспетчер логических дисков» отвечает за обнаружение (данная служба анализирует события службы «Plug and Play», возникающие при добавлении новых дисков) и наблюдение за новыми жесткими дисками, а также передачу информации о томах жестких дисков службе управления диспетчера логических дисков. Во всех рассматриваемых конфигурациях безопасности для указанной службы рекомендуется установить режим запуска «Вручную».

«Служба администрирования диспетчера логических дисков» выполняет настройку жестких дисков и томов. Данная служба выполняется только во время процессов настройки конфигурации жестких дисков и томов, после чего останавливается. Таким образом, во всех рассматриваемых конфигурациях безопасности режим запуска службы администрирования диспетчера логических дисков должен быть определен как «Вручную».

«Служба сообщений» осуществляет передачу и отправку сообщений службы «Оповещатель» между клиентскими и серверными компьютерами. Эта служба не имеет отношения к программе Windows Messenger и не является обязательной для компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003. По этим причинам во всех рассматриваемых конфигурациях безопасности службу сообщений необходимо отключить.

«Служба сетевого входа в систему» используется для проверки подлинности пользователей и служб и обеспечивает безопасный канал между компьютером и контроллером домена. Она передает на контроллер домена учетные данные пользователя, а возвращает идентификаторы безопасности пользователя и назначенные ему права. При

останове указанной службы компьютер под управлением ОС Microsoft® Windows Server™ 2003 R2 не сможет осуществлять проверку подлинности пользователей и служб, а контроллер домена осуществлять регистрацию DNS-записей. Запрещение данной службы на контроллер домена вызовет отказ осуществлять обработку NTLM-запросов аутентификации, что приведет к тому, что он будет недоступен для клиентских компьютеров. Таким образом, во всех рассматриваемых конфигурациях безопасности для службы сетевого входа в систему должен быть установлен автоматический режим запуска.

Служба «NetMeeting Remote Desktop Sharing» разрешает авторизованным пользователям с помощью программы Microsoft NetMeeting® получать удаленный доступ к компьютеру через корпоративную интрасеть. Чтобы запретить удаленный доступ пользователей к компьютерам, эту службу необходимо отключить. С целью обеспечения повышенного уровня безопасности, режим запуска данной службы во всех рассматриваемых конфигурациях должен соответствовать значению «Запрещен».

Служба «Сетевые подключения» управляет объектами папки «Сеть и удаленный доступ к сети», отображающей свойства локальной сети и подключений удаленного доступа. Если данная служба отключена, просмотр объектов локальной сети и удаленных подключений будет невозможен. Во всех рассматриваемых конфигурациях безопасности для указанной системной службы рекомендуется установить режим запуска «Вручную».

«Служба сетевого DDE» обеспечивает сетевой транспорт и безопасность динамического обмена данными (DDE) для программ, выполняющихся на одном или на разных компьютерах. Служба сетевого DDE, а также другие подобные автоматические сетевые службы могут использоваться нарушителями в своих целях. Поэтому с целью обеспечения требуемого уровня безопасности данная служба во всех рассматриваемых конфигурациях должна быть запрещена.

Служба «Диспетчер сетевого DDE» управляет сетевыми общими ресурсами динамического обмена данными DDE. Эта служба используется только службой сетевого DDE для управления общими каналами связи DDE. Диспетчер сетевого DDE, а также другие подобные автоматические сетевые службы могут служить объектами атак. Поэтому с целью обеспечения требуемого уровня безопасности режим запуска для данной службы во всех рассматриваемых конфигурации должен соответствовать значению «Запрещен».

«Служба сетевого расположения» собирает и хранит сведения о размещении и настройках вычислительной сети (таких как IP-адресация, изменения имени домена) и уведомляет приложения об их изменении. Поскольку во всех рассматриваемых конфигурациях безопасности может существовать необходимость использования

возможностей, обеспечиваемых данной службой, для нее рекомендуется установить режим запуска «Вручную».

Служба «Поставщик поддержки безопасности NTLM» обеспечивает безопасность программ, использующих механизм удаленного вызова процедур (RPC), через транспорты, отличные от именованных каналов, и позволяет пользователям осуществлять регистрацию в сети с использованием протокола аутентификации NTLM, что позволяет аутентифицировать клиентов, не поддерживающих Kerberos-аутентификацию. В случае если данная служба будет отключена, пользователи не смогут аутентифицироваться с помощью протокола NTLM и получить доступ к сетевым ресурсам. Следовательно, во всех рассматриваемых конфигурациях безопасности режим запуска службы «Поставщик поддержки безопасности NTLM» должен быть автоматический.

Служба «Журналы и оповещения производительности» управляет сбором данных о производительности с локального или удаленных компьютеров, выполняемым на основе заданного расписания, и обеспечивает запись этих данных в журналы или инициирует оповещение. Если эта служба остановлена, данные о производительности не собираются. Поскольку во всех рассматриваемых конфигурациях безопасности может существовать необходимость использования возможностей, обеспечиваемых данной службой, для нее рекомендуется установить режим запуска «Вручную».

Служба «Plug and Play» позволяет компьютеру распознавать изменения в установленном оборудовании и подстраиваться под них, либо не требуя вмешательства пользователя, либо сводя его к минимуму. Остановка или отключение этой службы может привести к нестабильной работе системы. Следовательно, во всех рассматриваемых конфигурациях безопасности режим запуска службы «Plug and Play» должен быть автоматический.

«Служба серийных номеров переносных устройств мультимедиа» обеспечивает получение серийных номеров переносного проигрывателя мультимедиа, подключенного к целевому компьютеру. Если данная служба остановлена, то защищенное содержимое может не загружаться на устройство. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Диспетчер очереди печати» управляет всеми локальными и сетевыми очередями печати, а также контролирует все задания печати. Диспетчер печати является ключевым компонентом системы печати в Windows. Он управляет очередями печати в системе, а также взаимодействует с драйверами принтеров и компонентами ввода-вывода,

например USB-портами и протоколами семейства TCP/IP. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования. Однако для серверов, реализующих роль серверов печати, данная служба должна иметь автоматический режим запуска.

Служба «Защищенное хранилище» обеспечивает защищенное хранение закрытых данных, таких, как закрытые ключи, для предотвращения несанкционированного доступа служб, процессов или пользователей. Если данная служба остановлена защищенное хранение данных не обеспечивает, что приводит к невозможности использования ряда механизмов безопасности. Следовательно, во всех рассматриваемых конфигурациях безопасности рекомендуется установить автоматический режим запуска службы «Защищенное хранилище».

Служба «Диспетчер автоматических подключений удаленного доступа» обеспечивает обнаружение неудачных попыток подключения к удаленной сети или удаленному компьютеру, а также предоставляет альтернативные методы подключения. Данная служба предлагает создать подключение к удаленной сети в случае неуспешной попытки обращения программы к удаленному DNS- или NetBIOS-имени или адресу. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Диспетчер подключений удаленного доступа» управляет подключениями удаленного доступа и подключениями виртуальных частных сетей к Интернету или другим вычислительным сетям. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Диспетчер сеанса справки для удаленного рабочего стола» управляет возможностями «Удаленного помощника» в Центре справки и поддержки операционной системы Microsoft® Windows Server™ 2003. После остановки данной службы «Удаленный помощник» будет недоступен. Чтобы обеспечить требуемый уровень безопасности во всех рассматриваемых конфигурациях безопасности данная служба должна быть отключена.

Служба «Удаленного вызова процедур (RPC)» представляет собой механизм взаимодействия между процессами (IPC), который позволяет осуществлять обмен данными и вызывать функции из других процессов. Другой процесс может быть запущен на локальном компьютере, в локальной сети или на удаленном компьютере; для получения доступа к нему используется подключение по глобальной (WAN) или виртуальной частной сети. Служба

RPC выступает в роли службы отображения конечных точек RPC и диспетчера служб COM (Component Object Model). Поскольку служба удаленного вызова процедур необходима для запуска многих других системных служб и работы многих программ и приложений во всех рассматриваемых конфигурациях безопасности для нее должен быть обеспечен автоматический режим запуска.

Служба «Локатор удаленного вызова процедур (RPC)» управляет базой данных службы имен RPC и позволяет клиентам службы удаленного вызова процедур использовать семейство API-функций RpcNs* API для обнаружения RPC-серверов. Данная служба должна быть включена, чтобы RPC-клиенты могли находить RPC-серверы. Поскольку во всех рассматриваемых конфигурациях безопасности не существует необходимости использования возможностей, обеспечиваемых данной службой, на рядовых серверах ее рекомендуется отключить.

Служба «Удаленный реестр» позволяет удаленным пользователям изменять параметры реестра на локальном компьютере при условии, что они имеют для этого необходимые права. В основном эта служба используется удаленными администраторами и счетчиками производительности. Отключение службы удаленного реестра ограничивает возможность изменения реестра только локальными пользователями, работающими на этом компьютере, и приведет к тому, что многие службы, зависящие от нее, не будут функционировать. При отключении данной службы администратор вынужден будет вручную управлять получением обновлений на каждом компьютере или обеспечить пользователям возможность самостоятельной установки обновлений. Таким образом, во всех рассматриваемых конфигурациях безопасности режим запуска службы «Удаленный реестр» должен соответствовать значению «Автоматически».

Служба «Съемные ЗУ» обеспечивает управление и систематизацию съемных носителей, а также управление автоматическими съемными носителями, а также поддерживает каталог идентификационной информации о каждом съемном устройстве, используемом на целевом компьютере. Поскольку во всех рассматриваемых конфигурациях безопасности может существовать необходимость использования возможностей, обеспечиваемых данной службой, для нее рекомендуется установить режим запуска «Вручную».

Служба «Поставщик результирующей политики» позволяет пользователю подключаться к удаленному компьютеру, получать доступ к базе данных инструментария управления Windows (WMI) этого компьютера, проверять либо текущие параметры групповой политики, применяемой для этого компьютера или пользователя, либо новые

параметры, перед тем как их применить. Если данная служба остановлена, удаленная проверка параметров групповой политики не обеспечивается. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Маршрутизация и удаленный доступ» обеспечивает услуги мультипротокольной маршрутизации в локальной и глобальной сетях, а также между сегментами сетей. Кроме того, данная служба предоставляет услуги удаленного доступа по коммутируемым и виртуальным частным вычислительным сетям. Для обеспечения требуемого уровня безопасности во всех рассматриваемых конфигурациях данная служба должна быть отключена.

Служба «Вторичного входа в систему» позволяет запускать процессы от имени другого пользователя. Данная возможность используется в случае необходимости временного повышения собственных привилегий для выполнения каких-либо административных задач. Служба вторичного входа в систему позволяет пользователю запускать процессы в ином контексте безопасности. Поскольку для большинства компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003, настроенных в соответствии с одной из рассматриваемых конфигураций безопасности, эти возможности не требуются, данная служба должна быть отключена.

«Диспетчер учетных записей безопасности» является защищенной подсистемой, обеспечивающей хранение и управление информацией об учетных записях пользователей и групп. Для корректного функционирования операционной системы во всех рассматриваемых конфигурациях безопасности режим запуска данной службы должен быть автоматический.

Системная служба «Сервер» обеспечивает поддержку удаленного вызова процедур, а также совместное использование файлов, принтеров и именованных каналов в сети. Служба сервера позволяет организовать совместное использование локальных ресурсов, например дисков и принтеров, с тем, чтобы к ним могли получать доступ другие пользователи сети, а также обмен данными по именованным каналам между программами на локальном и удаленных компьютерах. Если служба остановлена, такие функции не удастся выполнить. Таким образом, во всех рассматриваемых конфигурациях безопасности для данной службы должен быть определен автоматический режим запуска.

Служба «Определение оборудования оболочки» предоставляет уведомления для событий автоматического воспроизведения или выполнения «Автозапуск». Во всех

рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Смарт-карты» управляет доступом к устройствам чтения смарт-карт. Если эта служба остановлена, этот компьютер не сможет считывать смарт-карты. Если эта служба отключена, любые службы, которые явно зависят от нее, не могут быть запущены. Поскольку для компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003 R2, настроенных в соответствии с одной из рассматриваемых конфигураций безопасности, аутентификация пользователей с использованием смарт-карт не осуществляется, указанную службу рекомендуется отключить.

«Модуль поддержки специальной консоли администрирования» предоставляет администраторам удаленный доступ к командной строке с использованием службы аварийного управления в случаях получения ошибки STOP. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Уведомление о системных событиях» ведет наблюдение за системными событиями, обеспечивает их протоколирование и уведомляет подписчиков системы событий COM+ об этих событиях, рассылая оповещения. Во всех рассматриваемых конфигурациях безопасности для данной службы рекомендуется установить автоматический режим запуска.

Служба «Планировщик заданий» позволяет настраивать расписание автоматического выполнения задач на заданном компьютере. В тоже время его использование должно быть ограничено в средах с высокими требованиями к безопасности, что позволит предотвратить неправильное использование системных ресурсов или запуск злонамеренного кода. По этой причине, во всех рассматриваемых конфигурациях данная служба должна быть отключена.

Служба «Модуль поддержки NetBIOS через TCP/IP» обеспечивает поддержку службы NetBIOS через TCP/IP (NetBT) и разрешения NetBIOS-имен в адреса, тем самым обеспечивая доступ пользователей к общим папкам и принтерам. Во всех рассматриваемых конфигурациях безопасности для данной службы рекомендуется установить автоматический режим запуска.

Служба «Телефония» обеспечивает поддержку интерфейса Telephony API (TAPI) для программ, управляющих телефонным оборудованием и голосовой связью через протокол IP на целевом компьютере, а также через сеть - на серверах, где запущена соответствующая служба. Поскольку для большинства компьютеров под управлением операционной системы

Microsoft® Windows Server™ 2003, настроенных в соответствии с одной из рассматриваемых конфигураций безопасности, эти возможности не требуются, указанную службу рекомендуется отключить.

Служба «Telnet» предоставляет клиентам Telnet сеансы терминала ASCII. Эта служба предусматривает поддержку проверки подлинности и поддержку следующих типов терминалов: ANSI, VT-100, VT-52 и VTNT. Для большинства компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003, настроенных в соответствии с одной из рассматриваемых конфигураций безопасности, эти возможности не требуются. По этой причине во всех рассматриваемых конфигурациях безопасности служба «Telnet» должна быть отключена.

«Службы терминалов» обеспечивают многосеансовую среду для доступа клиентов к сеансам виртуального рабочего стола Windows и программам Windows, запущенным на сервере под управлением Microsoft® Windows Server™ 2003. Службы терминалов позволяют интерактивно подключиться к компьютеру нескольким пользователям. Поскольку указанная служба обеспечивает поддержку возможности удаленного администрирования серверов во всех рассматриваемых конфигурациях безопасности для нее необходимо установить автоматический режим запуска.

Системная служба «Лицензирования служб терминалов» производит установку сервера лицензий и предоставляет лицензии зарегистрированным пользователям, которые подключаются к серверу служб терминалов. Лицензирование служб терминалов - это служба, которая хранит выпущенные для сервера терминалов клиентские лицензии, а затем отслеживает лицензии, выданные клиентским компьютерам или терминалам. Для большинства компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003, настроенных в соответствии с одной из рассматриваемых конфигураций безопасности, эти возможности не требуются. По этой причине во всех рассматриваемых конфигурациях безопасности данная служба должна быть отключена

Системная служба «Каталога сеанса служб терминалов» позволяет кластерам серверов терминалов с балансировкой сетевой нагрузки правильно направлять пользовательский запрос на подключение к серверу, на котором уже запущен сеанс пользователя. Пользователь направляется на первый доступный сервер терминалов, независимо от того, запустил ли он уже другой сеанс в кластере серверов. С помощью сетевого протокола TCP/IP балансировка сетевой нагрузки производит объединение в общем пуле вычислительных мощностей нескольких серверов. Служба может быть использована в кластере серверов терминалов для повышения производительности отдельного сервера

путем распределения сеанса между несколькими серверами. Служба каталога сеанса служб терминалов отслеживает отключенные сеансы в кластере и обеспечивает повторное подключение пользователей к этим сеансам. Поскольку во всех конфигурациях безопасности рассмотренные возможности не используются данную службу «Каталога сеанса служб терминалов» рекомендуется отключить.

Служба «Темы» обеспечивает управление темами оформления. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Источник бесперебойного питания» управляет работой источников бесперебойного питания, подключенных к компьютеру. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить.

Служба «Диспетчер отгрузки» управляет синхронной и асинхронной передачей файлов между клиентами и серверами сети. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить.

«Служба виртуальных дисков» предоставляет набор унифицированных функций API, обеспечивающих управления программными и аппаратными томами. Поскольку во всех рассматриваемых конфигурациях безопасности в основном не существует необходимости использования указанных возможностей, обеспечиваемых данной службой, ее рекомендуется отключить.

Служба «Теневого копирования тома» управляет созданием теневых копий (контрольных точек состояния) дисковых томов, которые используются для архивации и восстановления или для иных целей. Если эта служба остановлена, теневые копии томов для восстановления не будут доступны и архивация и восстановление могут не работать. Поскольку во всех рассматриваемых конфигурациях безопасности может существовать необходимость использования возможностей, обеспечиваемых данной службой, для нее рекомендуется установить режим запуска «Вручную».

Служба «Веб-клиент» позволяет Win32-пиложениям создавать, получать доступ и изменять файлы, хранящиеся в Интернете. Поскольку во всех рассматриваемых конфигурациях безопасности не существует необходимости использования возможностей, обеспечиваемых данной службой, ее рекомендуется отключить.

Служба «Windows Audio» обеспечивает управление звуковыми устройствами для Windows-программ. Поскольку во всех рассматриваемых конфигурациях безопасности не существует необходимости использования возможностей, обеспечиваемых данной службой, ее рекомендуется отключить.

Служба «Windows Installer» позволяет добавлять, изменять и удалять приложения, предоставленные пакетом Windows Installer (*.msi). Поскольку указанная служба обеспечивает поддержку возможности управления приложениями во всех рассматриваемых конфигурациях безопасности для нее необходимо установить автоматический режим запуска.

«Инструментарий управления Windows» предоставляет общий интерфейс и объектную модель для доступа к информации об управлении операционной системой, устройствами, приложениями и службами. Поскольку после отключения данной службы многие Windows-приложения могут работать некорректно, во всех рассматриваемых конфигурациях безопасности для данной системной службы необходимо установить автоматический режим запуска.

«Служба времени Windows» управляет синхронизацией даты и времени на всех клиентах и серверах в сети. Если данная служба остановлена, возможности синхронизации даты и времени будут недоступны, что может привести к рассогласованию системного времени на компьютерах и, как следствие, к невозможности аутентификации пользователей с использованием протокола аутентификации Kerberos. Поэтому, во всех рассматриваемых конфигурациях безопасности для службы времени Windows необходимо установить автоматический режим запуска.

«Служба авто-обнаружения веб-прокси WinHTTP» реализует протокол автоматического обнаружения веб-прокси (Web Proxy AutoDiscovery, WPAD) для служб Windows HTTP (WinHTTP). Протокол WPAD позволяет клиентам HTTP автоматически определять параметры настройки прокси-сервера. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Беспроводная настройка» обеспечивает автоматическую настройку IEEE 802.11 адаптеров для беспроводной связи. Во всех рассматриваемых конфигурациях безопасности данную службу рекомендуется отключить по причине отсутствия необходимости ее использования.

Служба «Адаптер производительности WMI» предоставляет информацию о библиотеках производительности от поставщиков инструментария управления Windows (WMI HiPerf) клиентам сети. Данная служба работает по запросу только после активации библиотеки Performance Data Helper. Поскольку отключение службы «Адаптер производительности WMI» вызовет невозможность использования счетчиков

производительности WMI, во всех рассматриваемых конфигурациях безопасности для данной системной службы необходимо установить режим запуска «Вручную».

Служба «Рабочая станция» обеспечивает создание и поддержку клиентских сетевых подключений. Если данная служба остановлена, установление клиентских подключений к удаленным серверам и доступ к файлам данных с использованием именованных каналов будет невозможно. Таким образом, во всех рассматриваемых конфигурациях безопасности для службы «Рабочая станция» должен быть определен автоматический режим запуска.

«Служба веб-публикации» обеспечивает подключение и администрирование веб-узла с помощью оснастки IIS. Однако для большинства компьютеров под управлением операционной системы Microsoft® Windows Server™ 2003, настроенных в соответствии с одной из рассматриваемых конфигураций безопасности, эта служба не является обязательной. По этой причине во всех конфигурациях она должна быть запрещена.

А.2.2 Описание параметров безопасности, специфичных для серверов, выступающих в роли батион-хоста

В данном разделе представлены рекомендации по настройке механизмов защиты компьютеров под управлением ОС Microsoft® Windows Server™ 2003, выступающих в роли бастион-хоста, необходимые для обеспечения безопасной обработки на них конфиденциальной информации.

Как правило, бастион-хостом является компьютер, расположенный в общедоступной внешней вычислительной сети организации (демилитаризованной зоне) и обеспечивающий поддержку и предоставление различных видов услуг (таких как DNS, Web, FTP, SMTP, NNTP). В идеальном случае, бастион-хост должен реализовать только одну из указных функций, т.е. выступать, например, либо в роли веб-сервера, либо FTP-сервера. При совмещении бастион-хостом различных ролей возникают определенные трудности, связанные с их интеграцией, администрированием, конфигурированием, и как следствие повышается вероятность наличия в системе защиты брешей, позволяющих злоумышленникам успешно реализовывать различные атаки.

Для обеспечения безопасного функционирования бастион-хоста администратором, помимо настройки соответствующих параметров безопасности, должен быть выполнен ряд мероприятий, предусматривающих запрет/удаление служб, протоколов, программ и отключение сетевых интерфейсов, в которых нет необходимости.

Представленные ниже рекомендации позволят настроить бастион-хост в соответствии с конфигурацией безопасности «Specialized Security – Limited Functionality», которая позволит обеспечить требуемый уровень защищенности компьютеров, необходимый для обработки конфиденциальной информации, а также противостоять атакам нарушителей. Применяемые к компьютерам в роли бастион-хоста параметры безопасности определены в шаблоне безопасности `Specialized Security - Limited Functionality - Bastion Host.inf`.

Детальное описание всех параметров, определенных в указанном шаблоне безопасности, представлено в разделе А.2.1, поскольку настраиваемые для бастион-хостов параметры безопасности аналогичны тем, которые определяют требуемый уровень защищенности рядовых серверов (через политику Member Server Baseline Policy). В данном разделе представлено описание различий между параметрами безопасности, определяемыми локальной политикой безопасности компьютеров в роли бастион-хоста (Bastion Host Local Policy), и параметрами безопасности, определяемыми политикой Member Server Baseline Policy.

Параметры политики аудита

Параметры политики аудита, применяемые для компьютеров, выступающих в роли бастион-хоста, аналогичны параметрам политики аудита, определяемым для рядовых серверов политикой Member Server Baseline Policy (см. раздел А.2.1).

Параметры назначения прав пользователей

Параметры назначения прав пользователей, определяемые локальной групповой политикой, применяемой для компьютеров, выступающих в роли бастион-хоста, в большинстве своем аналогичны параметрам, определяемым для рядовых серверов политикой Member Server Baseline Policy (см. раздел А.2.1).

Ниже (см. таблицу А.2.2.1) представлены параметры назначения прав пользователей, значения которых отличаются от значений параметров, определяемых для рядовых серверов политикой Member Server Baseline Policy.

Таблица А.2.2.1 – Параметры назначения прав пользователей, используемые для обеспечения безопасности компьютеров, выступающих в роли бастион-хоста

№ п/п	Название параметра	Конфигурация безопасности «Specialized Security – Limited Functionality»
1.	Локальный вход в систему	Администраторы
2.	Отказ в доступе к компьютеру из сети	Анонимный вход, Встроенная учетная запись администратора, Support_388945a0, Гость

Право «Локальный вход в систему» определяет перечень пользователей, которые могут осуществлять интерактивный вход в систему. Учетная запись с правом локального входа в систему позволяет использовать для входа консоль компьютера. Ограничив число пользователей, которым разрешено локально входить в систему, можно предотвратить попытки несанкционированного доступа злоумышленников, предпринимаемых с целью компрометации бастион-хоста или вызова его отказа в обслуживании.

По умолчанию правом локального хода в систему обладают члены групп безопасности «Операторы учета», «Операторы архива», «Операторы печати» и «Опытные пользователи». Предоставление данного права только членам группы «Администраторы» позволит ограничить возможность административного доступа в систему пользователями с высоким уровнем доверия и компетентности, а также достичь требуемого уровня безопасности.

Назначение права «Отказ в доступе к компьютеру из сети» означает для пользователей запрет на доступ к данному компьютеру через сеть. Данное право запрещает использование ряда сетевых протоколов, включая протоколы SMB, NetBIOS, CIFS, HTTP и COM+. Данный параметр имеет больший приоритет по сравнению с параметром «Доступ к компьютеру из сети», если учетная запись пользователя контролируется обеими политиками.

В разделе А.2.1 данного руководства при описании параметров назначения прав пользователя для обеспечения наибольшего уровня безопасности указанное право рекомендуется назначать для группы «Гости». В тоже время, учтенная запись «IUSR» (используемая для анонимного доступа к веб-серверу IIS) по умолчанию является членом группы безопасности «Гости», что предполагает невозможность ее использования при доступе к бастион-хосту, если он реализует функции веб-сервера IIS. По этой причине, на серверах, выступающих в роли бастион-хоста, право «Отказ в доступе к компьютеру из сети» группе безопасности «Гости» не предоставляется. Таким образом, доступ к серверам

под управлением ОС Microsoft® Windows Server™ 2003, выступающим в роли бастион-хоста, должен быть ограничен только для встроенной учетной записи администратора, учетной записи «Гость», учетной записи «Support_388945a0», а также должны быть запрещены любые попытки анонимного доступа (учетная запись «Анонимный доступ»)[1].

Параметры безопасности

Параметры безопасности компьютеров, выступающих в роли бастион-хоста, аналогичны параметрам безопасности, определяемым на рядовых серверах политикой Member Server Baseline Policy (см. раздел А.2.1).

Параметры безопасности журналов регистрации событий

Параметры безопасности журналов регистрации событий, применяемые для бастион-хостов, аналогичны параметрам, определяемым в отношении журналов регистрации событий аудита на рядовых серверов политикой Member Server Baseline Policy (см. раздел А.2.1).

Системные службы

Серверы, выступающие в роли бастион-хоста, по своей природе подвержены внешним атакам. По этой причине, для каждого бастион-хоста должны быть предприняты определенные действия, которые позволят минимизировать область возможных атак. Чтобы соответствующим образом защитить бастион-хостом, администратором должно быть обеспечено отключение тех служб, которые не требуются для функционирования ОС, а также тех служб, которые не согласуются с возложенной на бастион-хост ролью (например, если бастион-хост реализует услуги электронной почты, то в функционировании на нем служб, обеспечивающих поддержку веб-сервера, нет необходимости).

В данном пункте представлено описание системных служб (см. таблицу А.2.2.2), которые должны быть запрещены на бастион-хостах под управлением ОС Microsoft® Windows Server™ 2003 с целью уменьшения области возможных атак, объектами которых данные службы могут выступать. При этом затрагиваются только те системные службы, режим запуска которых отличен от режима, определяемого политикой Member Server Baseline Policy, для компьютеров в конфигурации «Specialized Security – Limited Functionality» (см. раздел А.2.1).

Таблица А.2.2.2 – Параметры настройки системных служб для компьютеров, выступающих в

[1] Перечисленные учетные записи не включены в файлы шаблонов безопасности (за исключением учетной записи «Анонимный доступ») для соответствующих конфигураций безопасности, поскольку имеют уникальные для каждого домена Active Directory идентификаторы безопасности SID (Security Identifier). Таким образом, при настройке групповой политики они должны быть включены в соответствующие шаблоны безопасности администратором безопасности вручную.

роли бастион-хостов

№ п/п	Системная служба	Имя службы	Режим запуска службы в конфигурации «Specialized Security – Limited Functionality»
1.	Фоновая интеллектуальная служба передачи	BITS	Запрещен
2.	Обозреватель компьютеров	Browser	Запрещен
3.	DHCP-клиент	Dhcp	Запрещен
4.	Служба сетевого расположения	NLA	Запрещен
5.	Поставщик поддержки безопасности NTLM	NtLmSsp	Запрещен
6.	Журналы и оповещения производительности	SysmonLog	Запрещен
7.	Удаленный реестр	RemoteRegistry	Запрещен
8.	Сервер	lanmanserver	Запрещен
9.	Модуль поддержки NetBIOS через TCP/IP	LMHosts	Запрещен
10.	Службы терминалов	TermService	Запрещен
11.	Windows Installer	MSIServer	Запрещен
12.	Расширения драйверов WMI	Wmi	Запрещен
13.	Адаптер производительности WMI	WmiApSrv	Запрещен

«Фоновая интеллектуальная служба передачи» выполняет передачу данных в фоновом режиме, используя резервы сети по пропускной способности. BITS обеспечивает асинхронную передачу файлов между клиентом и HTTP-сервером, что позволяет улучшить скорость и устойчивость процесса передачи файлов, а также снизить загрузку сетевого подключения. В случае если эта служба остановлена, такие компоненты операционной системы, как Windows Update, «Автоматическое обновление» не смогут автоматически загружать программы и другие сведения. Это означает, что компьютер не сможет автоматически получать обновления от служб SUS (Software Update Services), если данная

служба сконфигурирована с использованием механизма групповой политики. Если служба BITS отключена, любые службы, которые явно зависят от нее, не могут быть запущены.

«Фоновая интеллектуальная служба передачи» не является обязательной для обеспечения функционирования бастион-хоста. Определение с использованием групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями и позволяет обеспечить ее настройку только уполномоченными администраторами. Кроме того, запрет запуска данной службы сужает область возможных атак. Таким образом, для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Служба «Обозреватель компьютеров» обслуживает список компьютеров в сети и выдает его программам по запросу. Кроме того, служба «Обозреватель компьютеров» используется компьютерами под управлением операционных систем семейства Microsoft Windows, которым необходимо просматривать сетевые ресурсы. Компьютеры, определенные в качестве обозревателей, поддерживают список, содержащий перечень всех совместно используемых ресурсов, доступных в сети.

Если служба «Обозреватель компьютеров» остановлена, список компьютеров в сети не будет создан или обновлен, а явно зависимые от нее службы не смогут быть запущены. Определение с использованием групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями и позволяет обеспечить ее настройку только уполномоченными администраторами. Кроме того, запрет запуска данной службы сужает область возможных атак. Таким образом, для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, рекомендуется запретить запуск указанной службы.

Служба «DHCP-клиент» управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен. Данная служба обеспечивает автоматическое получение клиентом IP-адреса и всех сетевых настроек (DNS, WINS) компьютера независимо от того, к какой вычислительной сети осуществлено подключение. В случае если данная служба остановлена, компьютеру не будет выделяться динамический IP-адрес и обеспечиваться динамическое обновление DNS. Таким образом, конфигурирование сетевых настроек должно будет осуществляться администратором вручную. Если служба «DHCP-клиент» отключена, любые службы, которые явно зависят от нее, не могут быть запущены.

Служба «DHCP-клиент» не является обязательной для обеспечения функционирования бастион-хоста. Определение с использованием групповой политики

режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями и позволяет обеспечить ее настройку только уполномоченными администраторами. Кроме того, запрет запуска данной службы сужает область возможных атак. По этим причинам для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

«Служба сетевого расположения» собирает и хранит сведения о размещении и настройках вычислительной сети (таких как IP-адресация, изменения имени домена) и уведомляет приложения об их изменении.

Данная служба не является обязательной для обеспечения функционирования бастион-хоста. Определение с использованием групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями. Кроме того, запрет запуска данной службы сужает область возможных атак. По этим причинам для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Служба «Поставщик поддержки безопасности NTLM» обеспечивает безопасность программ, использующих механизм удаленного вызова процедур (RPC), через транспорты, отличные от именованных каналов, и позволяет пользователям осуществлять регистрацию в сети с использованием протокола аутентификации NTLM, что позволяет аутентифицировать клиентов, не поддерживающих Kerberos-аутентификацию. В случае если данная служба будет отключена, пользователи не смогут аутентифицироваться с помощью протокола NTLM и получить доступ к сетевым ресурсам.

Данная служба не является обязательной для обеспечения функционирования бастион-хоста. Кроме того, запрет запуска данной службы сужает область возможных атак. Следовательно, для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Служба «Журналы и оповещения производительности» управляет сбором данных о производительности с локального или удаленных компьютеров, выполняемым на основе заданного расписания, и обеспечивает запись этих данных в журналы или инициирует оповещение. Останов указанной службы приведет к тому, что сбор данных о производительности собираться не будет, запущенные процессы сбора информации будут остановлены, а запланированные задания сбора информации не будут запущены.

Данная служба не является обязательной для обеспечения функционирования бастион-хоста. Кроме того, запрет запуска данной службы сужает область возможных атак, направленных против бастион-хоста. Следовательно, для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Служба «Удаленный реестр» позволяет удаленным пользователям изменять параметры реестра на локальном компьютере при условии, что они имеют для этого необходимые права. Только членам групп безопасности «Администраторы» и «Операторы архива» по умолчанию предоставлено данное право удаленного доступа к реестру. В основном эта служба используется удаленными администраторами и счетчиками производительности. Отключение службы удаленного реестра ограничивает возможность изменения реестра только локальными пользователями, работающими на этом компьютере, и приведет к тому, что многие службы, зависящие от нее, не будут функционировать. При отключении данной службы администратор вынужден будет вручную управлять получением обновлений на каждом компьютере или обеспечить пользователям возможность самостоятельной установки обновлений.

Служба «Удаленный реестр» не является обязательной для обеспечения функционирования бастион-хоста. Определение с использованием групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями. Кроме того, запрет запуска данной службы сужает область возможных атак. По этим причинам для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Системная служба «Сервер» обеспечивает поддержку удаленного вызова процедур, а также совместное использование файлов, принтеров и именованных каналов в сети. Служба сервера позволяет организовать совместное использование локальных ресурсов, например дисков и принтеров, с тем, чтобы к ним могли получать доступ другие пользователи сети, а также обмен данными по именованным каналам между программами на локальном и удаленном компьютерах. Если служба сервера остановлена, такие функции не удастся выполнить, а все службы, которые явно зависят от нее, не смогут быть запущены.

Служба сервера не является обязательной для обеспечения функционирования бастион-хоста, поскольку обеспечение функций поддержки совместно используемых ресурсов являются нетипичными для него. Определение с использованием групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее

злоумышленного конфигурирования нарушителями. Кроме того, запрет запуска данной службы сужает область возможных атак. По этим причинам для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, служба сервера должна быть запрещена.

Служба «Модуль поддержки NetBIOS через TCP/IP» обеспечивает поддержку службы NetBIOS через TCP/IP (NetBT) и разрешения NetBIOS-имен в адреса, тем самым обеспечивая доступ пользователей к общим папкам и принтерам. Служба «Модуль поддержки NetBIOS через TCP/IP» также обеспечивает поддержку службы NetBT, выполняя разрешение имен DNS и осуществляя проверку доступности адресатов, по результатам которой возвращается список IP-адресов доступных сетевых узлов.

Если данная служба остановлена, такие функции не удастся выполнить, а все службы, которые явно зависят от нее, не смогут быть запущены. Кроме того, останов данной службы приведет к невозможности использования групповой политики, базируемой на Active Directory. Служба «Модуль поддержки NetBIOS через TCP/IP» не является обязательной для обеспечения функционирования бастион-хоста. Определение с использованием локальной групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями. По этим причинам для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен. Кроме того, запрет запуска данной службы сужает область возможных атак.

«Службы терминалов» обеспечивают многосеансовую среду для доступа клиентов к сеансам виртуального рабочего стола Windows и программам Windows, запущенным на сервере под управлением Microsoft® Windows Server™ 2003. Данная служба обеспечивает поддержку возможности удаленного администрирования серверов.

«Службы терминалов» не являются обязательными для обеспечения корректного функционирования бастион-хоста. Определение с использованием групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями. Кроме того, запрет запуска данной службы сужает область возможных атак. Таким образом, для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Служба «Windows Installer» позволяет добавлять, изменять и удалять приложения, предоставленные пакетом Windows Installer (*.msi). «Windows Installer» является не только программой установки, она также обеспечивает функции системы

управления программным обеспечением, осуществляя инсталляцию, добавление и удаление компонент ПО. Дополнительно, служба «Windows Installer» поддерживает возможность установки и запуска программ из множественных источников и может быть использована сторонними разработчиками для инсталляции ими собственных приложений.

В случае определения для данной службы режима запуска «Вручную» приложения, которым необходим инсталлятор, смогут осуществлять запуск «Windows Installer». В случае если служба «Windows Installer» остановлена, все операции по установке, удалению, восстановлению и модификации, базирующиеся на «Windows Installer», будут невозможны, а другие службы, которые явно зависят от данной службы, не смогут быть запущены.

Служба «Windows Installer» не является обязательной для обеспечения функционирования бастион-хоста. Определение с использованием групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями. Кроме того, запрет запуска данной службы сужает область возможных атак. По этим причинам для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Служба «Расширения драйверов WMI» обеспечивает обмен управляющей информацией с устройствами, мониторинг всех драйверов и поставщиков трассировок событий (event trace providers).

Служба «Расширения драйверов WMI» не является обязательной для обеспечения функционирования бастион-хоста. Кроме того, запрет запуска данной службы сужает область возможных атак. По этим причинам для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Служба «Адаптер производительности WMI» предоставляет информацию о библиотеках производительности от поставщиков WMI HiPerf. Приложения и службы, которым необходимо предоставить счетчики производительности, могут воспользоваться двумя способами: обратиться к поставщикам WMI HiPerf или библиотекам производительности. Служба «Адаптер производительности WMI» преобразует счетчики производительности, предоставляемые поставщиками WMI HiPerf, в счетчики, которые могут быть задействованы PDH-клиентами (Performance Data Helper), например, приложением Sysmon, через библиотеку производительности RAP (Reverse Adapter Performance).

В случае если служба «Адаптер производительности WMI» будет остановлена, счетчики производительности WMI станут недоступными, а другие службы, которые явно зависят от указанной службы, не смогут быть запущены. Служба «Адаптер производительности WMI» не является обязательной для обеспечения функционирования бастион-хоста. Определение с использованием групповой политики режима запуска данной службы позволяет предотвратить возможные попытки ее злоумышленного конфигурирования нарушителями. Кроме того, запрет запуска данной службы сужает область возможных атак. По этим причинам для обеспечения безопасного функционирования серверов, выступающих в роли бастион-хоста, запуск указанной службы должен быть запрещен.

Дополнительные настройки безопасности

Осуществляемые для компьютеров, выступающих в роли бастион-хоста, дополнительные настройки безопасности предусматривают удаление сетевых протоколов и привязок, в которых нет необходимости.

На компьютерах, доступных из сетей общего пользования (например, Интернет), должны быть запрещены все сетевые протоколы, которых не используются. Это позволит противостоять различным угрозам, объектами которых они могут выступать. В частности, данные атаки могут быть направлены на получение необходимой информации относительной атакуемой системы с целью поиска в ней дополнительных уязвимостей. Так, SMB-протокол позволяет пользователям, не прошедшим процедуру аутентификации, получать в рамках null-сессии информацию относительно общих папок, учетных записях пользователей системы (включая информацию о членстве в группах безопасности и назначенных правах), ключах реестра и т.д.

Запрет SMB-протокола и службы NetBIOS через TCP/IP позволяет повысить безопасность бастион-хоста, существенно снизив при этом область возможных атак. Хотя настройка сервера в соответствии с описанной выше конфигурацией безопасности приведет к ухудшению управляемости системы и невозможности доступа к расположенным в вычислительной сети общим папкам, в тоже время эти меры позволяют обеспечить эффективную защиту сервера от различных угроз безопасности.

Чтобы отключить поддержку системой протокола SMB, должны быть выполнены следующие действия:

1. Осуществлен вызов свойств сетевого подключения к сети общего пользования. Для этого нажать Пуск → Панель управления → Сетевые подключения. Далее выбрать требуемое сетевое подключение и вызвать диалоговое окно его свойств.

2. В диалоговом окне свойств подключения в группе «Компоненты, используемые этим подключением» выбрать элемент «Клиент для сетей Microsoft» и нажать «Удалить» (см. рисунок А.2.2.1).

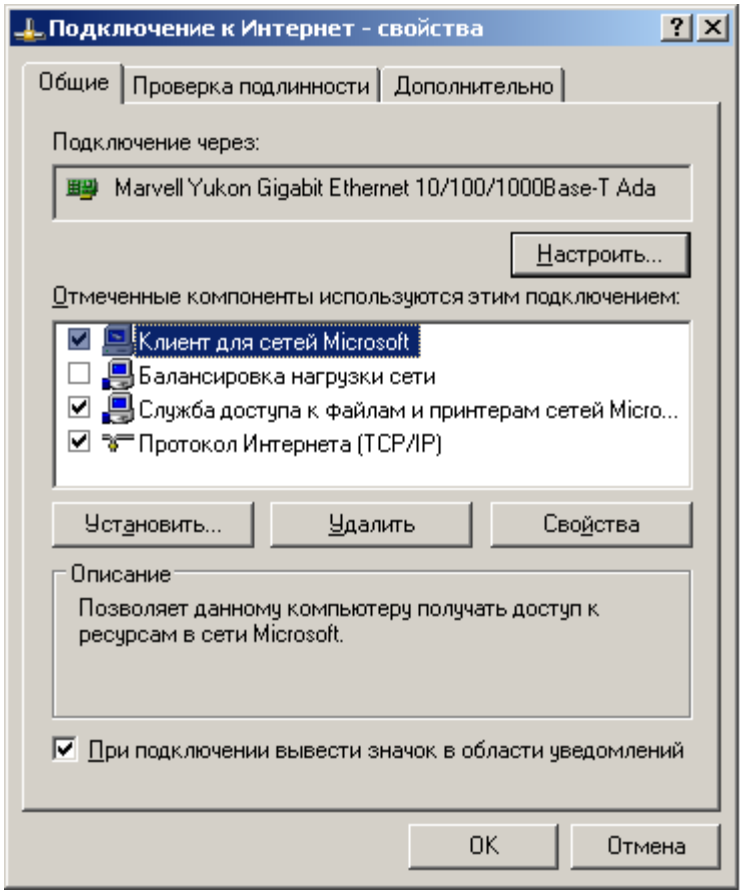


Рисунок А.2.2.1

3. Далее выбрать элемент «Служба доступа к файлам и принтерам сетей Microsoft» и нажать «Удалить».

4. Закрыть диалоговое окно свойств сетевого подключения.

Чтобы отключить поддержку операционной системой службы NetBIOS через TCP/IP (NetBIOS over TCP/IP), должны быть выполнены следующие действия:

1. Осуществлен вызов «Диспетчера устройств». Для этого нажать Пуск → Панель управления → Система. В появившемся диалоговом окне свойств системы перейти на вкладку «Оборудование» и нажать «Диспетчер устройств».

2. В диалоговом окне диспетчера устройств выбрать меню «Вид» и далее пункт «Показать скрытые устройства».

3. В появившемся списке раскрыть элемент «Драйверы устройств не Plug-n-Play».

5. Выбрать «NetBIOS через TCP/IP» и далее через контекстное меню «Отключить» (см. рисунок А.2.2.2).

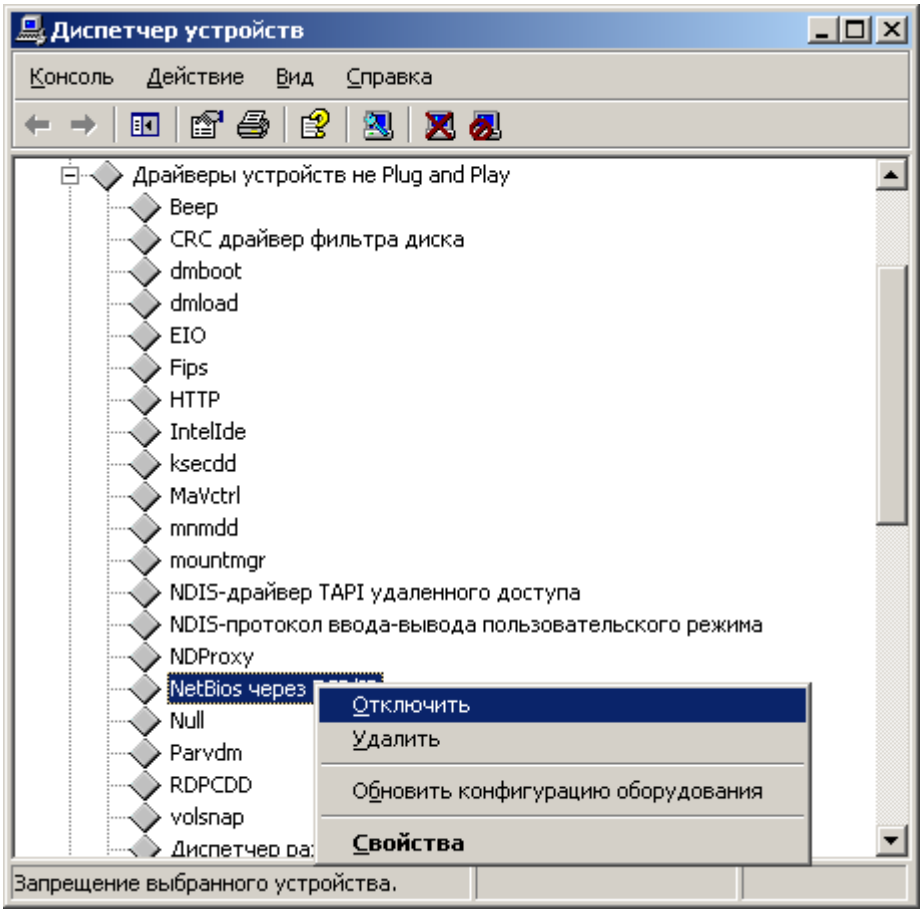


Рисунок А.2.2.2

4. Закрыть диалоговое окно диспетчера устройств.

Приложение Б

Б.1 Общие положения по подготовке к аттестации объектов информатизации по требованиям безопасности

Началу обработки конфиденциальной информации на объекте информатизации должна предшествовать его подготовка и аттестация на соответствие требованиям по безопасности информации, изложенным в законодательных, нормативных, правовых и руководящих документах, действующих на момент проведения аттестации.

Подготовка объекта информатизации к аттестации предусматривает:

1. Создание системы (подсистемы) информационной безопасности организации, эксплуатирующей объект информатизации.
2. Создание системы защиты конфиденциальной информации объекта информатизации.
3. Организацию безопасной эксплуатации объекта информатизации и поддержание его системы защиты информации в актуальном состоянии.

Аттестация объекта информатизации выполняется специальной комиссией (экспертной группой), создаваемой внутри организации, эксплуатирующей объект информатизации, с привлечением компетентных специалистов в области защиты информации.

Аттестация объекта информатизации может проводиться на договорной основе силами сторонней организации, специализирующейся в области защиты информации и имеющей соответствующие лицензии по защите конфиденциальной информации.

В ходе проведения аттестации экспертной комиссией проводится оценка достаточности и эффективности реализованных на объекте информатизации организационных и технических мер по защите конфиденциальной информации.

По результатам работы аттестационной комиссии на объект информатизации выдается специальный документ – «Аттестат соответствия объекта информатизации требованиям по безопасности информации» [1].

Система (подсистема) информационной безопасности организации должна включать:

- подразделения (специалистов) по защите информации;
- комплект организационно-распорядительных и плановых документов по защите информации;

– общеобъектовые системы обеспечения безопасности, включая системы охраны, видеонаблюдения и контроля доступа, системы пожарной безопасности и др.

Формирование *подразделения по защите информации* предполагает определение его функциональных задач, полномочий и зон ответственности, обучение персонала и назначение на должности приказами соответствующих руководителей.

При этом ответственность за выполнение требований по технической защите конфиденциальной информации возлагается на руководителей организаций, эксплуатирующих объекты информатизации. Организация работ по защите информации возлагается на руководителей подразделений, осуществляющих разработку проектов объектов информатизации и их эксплуатацию, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации - на руководителей подразделений по защите информации (служб безопасности) организации.

Комплект организационно-распорядительных и плановых документов по защите информации в организации в целом должен определять:

– политику информационной безопасности организации;
– порядок доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации;
– организацию физической защиты помещений и собственно технических средств обработки информации с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации;
– порядок учета и надежного хранения бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение (носители конфиденциальной информации на магнитной (магнитооптической), оптической и бумажной основе должны учитываться, храниться и уничтожаться в подразделениях организации в установленном порядке);
– разрешительную систему доступа персонала к конфиденциальным сведениям;
– сведения конфиденциального характера, подлежащие защите в организации;
– систему конфиденциального документооборота, включая порядок учета носителей конфиденциальной информации;

- порядок планирования и проведения работ по созданию и эксплуатации объектов информатизации и их средств защиты информации в организации;
- порядок контроля состояния защиты информации в организации, проводимого с целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к ней и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности или доступности информации;
- ответственность персонала за нарушение требований информационной безопасности.

Как правило, комплект организационно-распорядительных и плановых документов по защите информации применительно к организации включает:

- перечень сведений конфиденциального характера, подлежащих защите в организации в соответствии с законодательными и нормативными правовыми актами, а также другими внутренними (внутриведомственными) документами;
- документы, определяющие политику безопасности организации в части общей разрешительной системы доступа различных категорий персонала к конфиденциальным сведениям и порядок предоставления пользователям установленных полномочий доступа к соответствующим видам информации, обрабатываемой на объектах информатизации (например, концепция информационной безопасности организации);
- инструкцию по организации служебного документооборота;
- «Положение о порядке организации и проведения работ по защите конфиденциальной информации», содержащее:
  - порядок определения защищаемой информации;
  - порядок привлечения подразделений организации, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и СЗИ, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;
  - порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
  - порядок разработки, ввода в действие и эксплуатацию объектов информатизации;

- ответственность должностных лиц за своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗИ;

– положение по контролю состояния защиты информации;

– положение о подразделении (специалисте) по защите информации.

Система защиты конфиденциальной информации объекта информатизации включает две основные подсистемы:

1. Подсистему защиты информации от несанкционированного доступа (НСД).

2. Подсистему защиты информации от утечки или воздействия на нее по техническим каналам (реализуется при необходимости и в данном руководстве не рассматривается).

Подсистему защиты информации от несанкционированного доступа образуют:

– сертифицированные средства защиты информации от НСД;

– организационно-распорядительные и эксплуатационные документы;

– персонал, обеспечивающий безопасную эксплуатацию объекта информатизации и поддержание его системы защиты информации в актуальном состоянии (администратор информационной безопасности, администратор сети, пользователи и др.).

Соответствующим образом настроенная сертифицированная версия операционной системы Microsoft® Windows Server™ 2003 в совокупности с сертифицированными средствами доверенной загрузки может рассматриваться в качестве сертифицированного средства защиты информации от НСД, достаточного для построения автоматизированных систем до класса защищенности 1Г включительно.

При этом средства защиты информации от НСД и их настройки должны обеспечивать:

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации, а также к носителям информации на магнитной (магнитооптической), оптической и бумажной основе в соответствии с разработанной и утвержденной разрешительной системой допуска к сведениям конфиденциального характера, действующей в организации. При этом права и полномочия доступа пользователей к информации, обрабатываемой на объекте

информатизации, реализуются на основе соответствующих групповых политик или матрицы доступа;

- регистрацию действий пользователей и обслуживающего персонала при проведении работ на объекте информатизации, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- регулярное дублирование (резервное копирование) массивов и носителей информации;
- предотвращение внедрения программ-вирусов, программных закладок.

В качестве дополнительных организационных и технических мер по защите конфиденциальной информации на объекте информатизации рекомендуются:

- использование средств «гарантированной загрузки» операционной системы;
- регистрация выдачи печатных (графических) документов на «твердую» копию;
- учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал;
- учет обеспечение учета в журнале (картотеке) с регистрацией их выдачи (приема);
- использование средств восстановления операционной системы после сбоя;
- обеспечение защиты технических средств, на базе которых функционирует операционная система, от несанкционированной физической модификации;
- управление настройками безопасности операционной системы администраторами безопасности;
- размещение объектов защиты на максимально возможном расстоянии от границы контролируемой зоны;
- размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;
- использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
- использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания);
- применение средств защиты от утечки информации или воздействия на нее по техническим каналам.

Для передачи информации по каналам связи, выходящим за пределы контролируемой зоны, рекомендуется использовать защищенные каналы связи, в том числе защищенные

волоконно-оптические линии связи, а при использовании открытых каналов связи, применять сертифицированные криптографические средства защиты информации.

Совокупность организационно-распорядительных и эксплуатационных документов на аттестуемый объект информатизации должна определять:

- класс защищенности объекта информатизации;
- состав технических и программных средств, установленных на аттестуемом объекте информатизации;
- установленную технологию (описание технологического процесса) обработки информации на объекте информатизации;
- порядок обращения с защищаемыми информационными ресурсами (порядок их учета, хранения, обработки, передачи во внешние сети и другие организации);
- основные права, обязанности и порядок работы пользователей и администраторов;
- права доступа к защищаемым информационным ресурсам и порядок их получения;
- порядок установки и внесения изменений в состав технических и программных средств и регламент их обслуживания и сопровождения;
- порядок организации антивирусной защиты;
- порядок организации резервного копирования и восстановления информации;
- ответственность за нарушение установленного порядка работ на объекте информатизации.

Данные документы реализуются в виде:

- акта классификации автоматизированной системы (объекта информатизации);
- паспорта (формуляра) объекта;
- различного рода приказов, положений, инструкций и других видов и форм организационно-распорядительных документов.

Организация безопасной эксплуатации объекта информатизации и поддержание его системы защиты информации в актуальном состоянии предполагает:

- определение (назначение) должностных лиц, ответственных за эксплуатации объекта информатизации и его системы защиты информации;
- обучение персонала;
- оперативное изменение прав доступа пользователей к защищаемым информационным ресурсам;

– организацию антивирусной защиты, резервного копирования и восстановления информации;
– установку и внесение изменений в состав технических и программных средств;
– организацию контроля за состоянием защиты информации на объекте информатизации, включая анализ действий пользователей и обслуживающего персонала при проведении работ на объекте информатизации, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц.

Б.2 Порядок подготовки к аттестации объектов информатизации по требованиям безопасности

Подготовка к аттестации автономных рабочих мест на базе ПЭВМ с установленной сертифицированной версией операционной системы Microsoft® Windows Server™ 2003 проводится в следующей последовательности:

1. Провести экспертное обследование объекта информатизации.
2. Определить класс защищенности автоматизированной системы [1,2].
3. Установить операционную систему Microsoft® Windows Server™ 2003 и настроить ее в соответствии с той конфигурацией, в которой данное изделие было сертифицировано (см. раздел 2), осуществить контроль версии и текущих настроек безопасности операционной системы (см. раздел 3).
4. Реализовать дополнительные условия эксплуатации операционной системы.
5. Установить необходимое общесистемное и прикладное программное обеспечение, включая средства антивирусной защиты.
6. Убедиться в наличии и эффективности функционирования системы (подсистемы) информационной безопасности организации, эксплуатирующей объект информатизации.
7. Разработать необходимые организационно-распорядительные и эксплуатационные документы по защите информации на объект информатизации.
8. Сформировать матрицу прав доступа пользователей к информационным ресурсам автоматизированной системы и выполнить соответствующие настройки операционной системы, программных приложений и используемых средств защиты от НСД. Настройка разграничения доступа пользователей и обслуживающего персонала к информационным ресурсам системы осуществляется в следующей последовательности:

– посредством контекстного меню необходимо получить доступ к диалоговому окну свойств защищаемого информационного ресурса (файла или папки) и перейти на вкладку «Безопасность» (см. рисунок Б.2.1);

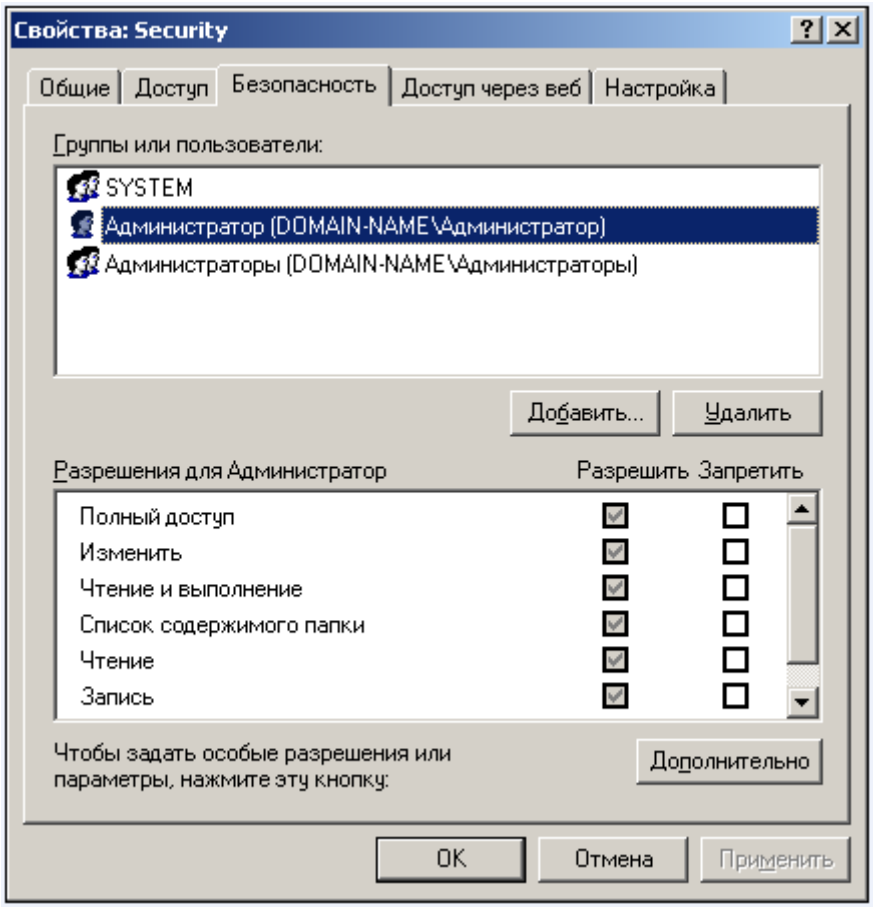


Рисунок Б.2.1

– через кнопку «Добавить…» выбрать пользователей или группы пользователей (субъектов доступа), которым необходимо запретить или предоставить разрешения на доступ к данному ресурсу (объекту доступа) (см. рисунок Б.2.2):

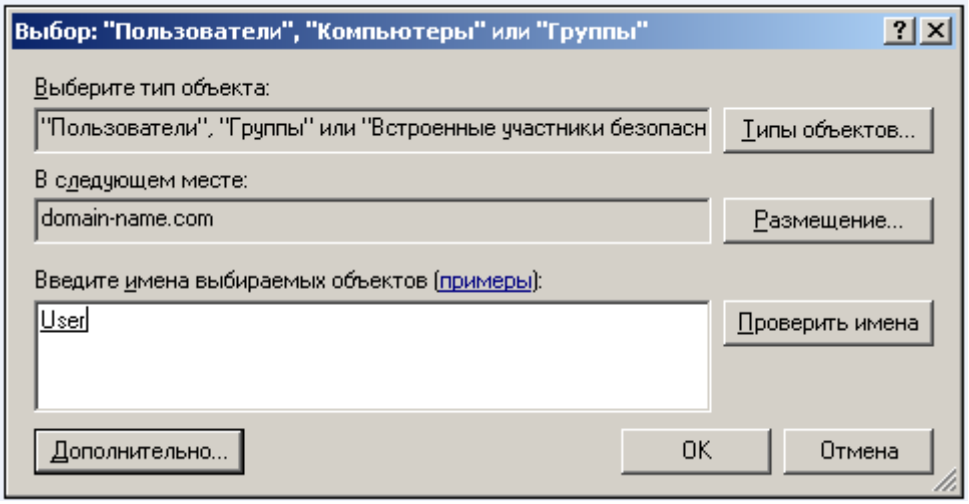


Рисунок Б.2.2

– в окне списка разрешений, установить или снять соответствующий флажок, чтобы явно разрешить или запретить доступ к ресурсу выбранным пользователям или группам пользователей. С целью более гибкой настройки разрешений на доступ к защищаемому ресурсу через кнопку «Дополнительно» окна свойств защищаемого информационного ресурса получить доступ к окну настройки дополнительных параметров безопасности (см. рисунок Б.2.3). Через кнопку «Изменить…» получить доступ к диалоговому окну «Элемент разрешений для …» и установить требуемые разрешения доступа для выбранных субъектов (см. рисунок Б.2.4).

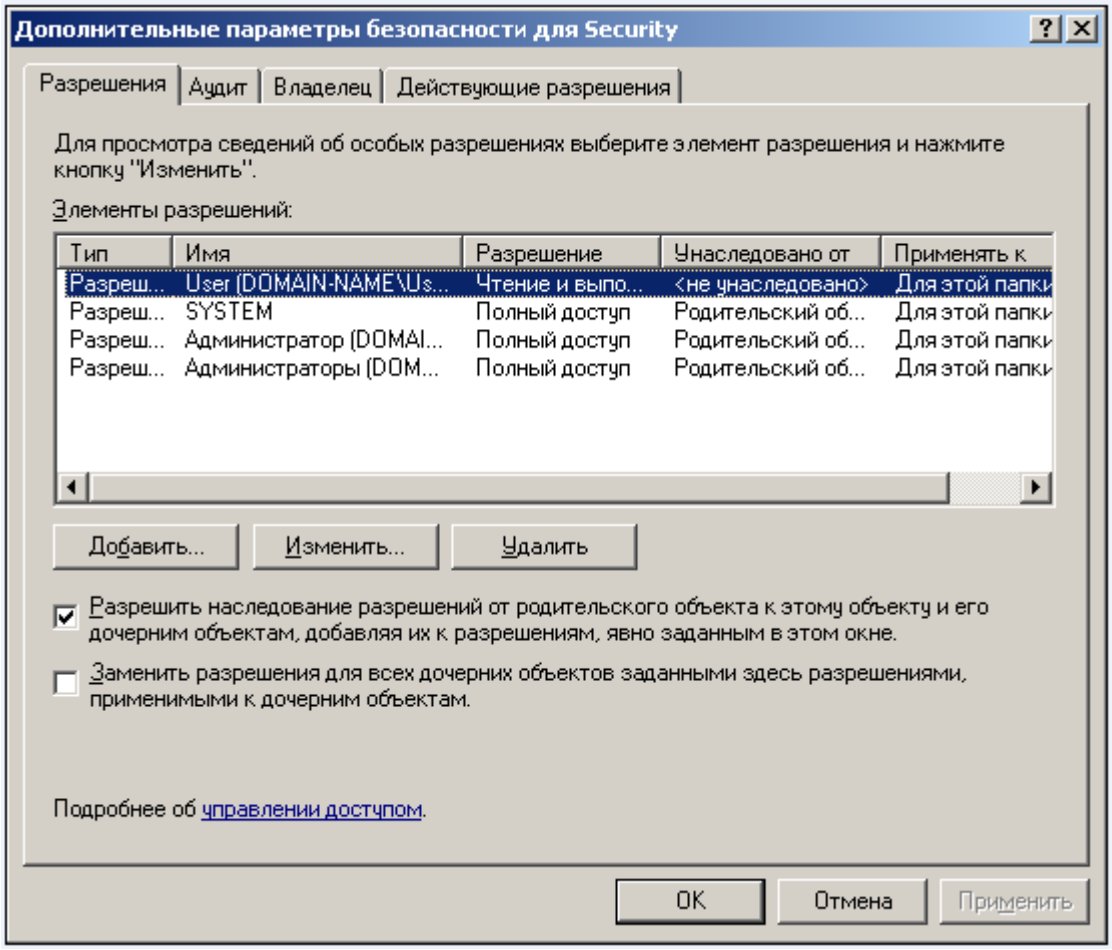

Дополнительные параметры безопасности для Security
Разрешения
Аудит
Владелец
Действующие разрешения
Для просмотра сведений об особых разрешениях выберите элемент разрешения и нажмите кнопку "Изменить".
Элементы разрешений:
Тип
Имя
Разрешение
Унаследовано от
Применять к
Разреш... User (DOMAIN-NAME\Us... Чтение и выпо... <не унаследовано> Для этой папки
Разреш... SYSTEM Полный доступ Родительский об... Для этой папки
Разреш... Администратор (DOMAI... Полный доступ Родительский об... Для этой папки
Разреш... Администраторы (DOM... Полный доступ Родительский об... Для этой папки
Добавить...
Изменить...
Удалить
Разрешить наследование разрешений от родительского объекта к этому объекту и его дочерним объектам, добавляя их к разрешениям, явно заданным в этом окне.
Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам.
Подробнее об управлении доступом.
OK
Отмена
Применить

Рисунок Б.2.3

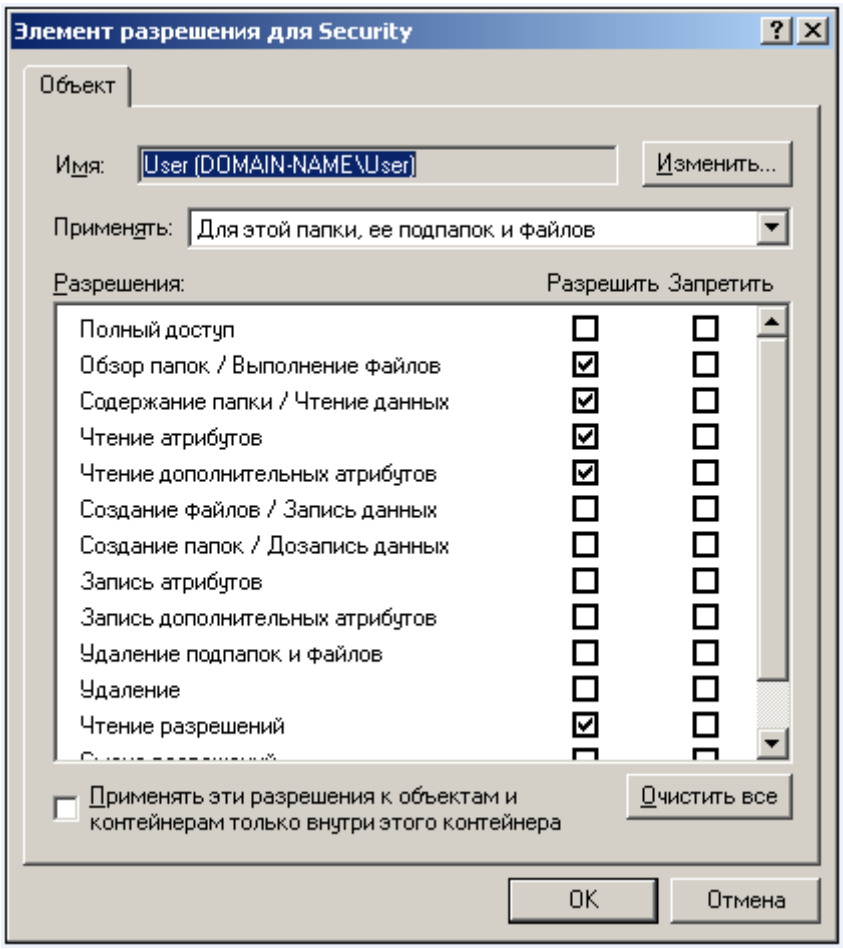


Рисунок Б.2.4

9. Провести проверку функционирования подсистемы управления доступом (механизмы идентификации, аутентификации и контроля доступа), подсистемы регистрации и учета, подсистемы обеспечения целостности [2].

10. Оценить уровень подготовки персонала (знание организационно-распорядительных и эксплуатационных документов по защите информации на объект информатизации) и распределение ответственности за выполнение требований по защите информации.

11. Убедиться в наличии и эффективном функционировании системы безопасной эксплуатации объекта информатизации и поддержании его системы защиты информации в актуальном состоянии.

12. Подготовить аттестат соответствия на объект информатизации и приложения к нему (для автоматизированного формирования и печати «Аттестата соответствия …» может использоваться «Программа контроля сертифицированной версии Microsoft® Windows Server™ 2003», поставляемая на компакт-диске дополнительно к дистрибутиву операционной системы Microsoft® Windows Server™ 2003).