

**ОПЕРАЦИОННАЯ СИСТЕМА  
MICROSOFT® WINDOWS® XP PROFESSIONAL**

**РУКОВОДСТВО ПО БЕЗОПАСНОЙ НАСТРОЙКЕ И КОНТРОЛЮ  
СЕРТИФИЦИРОВАННОЙ ВЕРСИИ**

## Оглавление

1 Введение.....	4
2 Последовательность действий по настройке сертифицированной версии операционной системы Microsoft® Windows® XP Professional.....	7
2.1 Общие указания по настройке параметров безопасности сертифицированной версии операционной системы Microsoft® Windows® XP Professional.....	7
2.2.1 Настройка клиентского компьютера, являющегося членом домена Active Directory в конфигурации «High Security» или «Enterprise».....	9
2.2.2 Настройка автономного компьютера в конфигурации «High Security» или «Enterprise», функционирующего в домене Active Directory, Windows NT 4.0 или полностью автономно.....	13
2.3 Порядок отключения функции автоматического обновления операционной системы Microsoft® Windows® XP Professional .....	16
2.4 Порядок отключения возможности самостоятельной смены пароля пользователем.....	23
2.5 Настройка рекомендуемых параметров безопасности брандмауэра Windows 25	
3 Последовательность действий по контролю сертифицированной версии операционной системы Microsoft® Windows® XP Professional.....	30
3.1 Контроль маркирования сертифицированной версии операционной системы Microsoft® Windows® XP Professional.....	30
3.2 Автоматизированный контроль сертифицированной версии операционной системы Microsoft® Windows® XP Professional .....	30
Установка и запуск на выполнение программы «XP_Check».....	31
Выполнение программы «XP_Check».....	36
3.3 Поиск и диагностика неисправностей программы «XP_Check».....	44
Приложение А.....	46
А.1 Групповая политика.....	46
А.2 Рекомендованные параметры безопасности клиентских компьютеров под управлением операционной системы Microsoft® Windows® XP Professional ...	47
Приложение Б .....	101
Б.1 Общие положения по подготовке к аттестации объектов информатизации по требованиям безопасности.....	101

Б.2	Порядок подготовки к аттестации объектов информатизации по требованиям безопасности.....	106
Приложение В.....		111
В.1	Рекомендованные значения параметров безопасности брандмауэра Windows .....	111

## **1 Введение**

Настоящий документ содержит рекомендации по настройке и контролю механизмов защиты операционной системы Microsoft® Windows® XP Professional при организации обработки конфиденциальной информации на объекте информатизации.

Руководство предназначено для настройки механизмов защиты операционной системы Microsoft® Windows® XP Professional в соответствии с той конфигурацией, в которой данное программное обеспечение было сертифицировано, а также подготовки объекта информатизации к аттестации на соответствие требованиям безопасности при обработке конфиденциальной информации (см. Приложение Б).

Операционная система Microsoft® Windows® XP Professional может функционировать как на автономном компьютере, так и на компьютере в составе локальной вычислительной сети. В свою очередь в локальной вычислительной сети может быть развернута инфраструктура службы каталогов Microsoft® Active Directory™ на базе операционных систем семейства Microsoft® Windows Server 2003™, Microsoft® Windows® 2000 или Microsoft® Windows 2008 Server™. В этом случае компьютер с установленной на нем операционной системой Microsoft® Windows® XP Professional может быть включен в состав домена Active Directory (и таким образом, централизованное управление политиками безопасности для него будет осуществляться контроллером домена), либо не входить в него, но иметь возможность взаимодействовать с другими компьютерами в составе домена. Взаимодействие компьютера в данной конфигурации с остальными будет эквивалентно взаимодействию компьютеров в составе рабочей группы (Workgroup).

Кроме того, компьютер с установленной на нем операционной системой Microsoft® Windows® XP Professional может быть включен в домен на базе предшествующих версий серверных операционных систем (Microsoft Windows NT® 4.0). В этом случае клиентский компьютер будет функционировать так же как автономный, и управление параметрами безопасности в этом случае будет осуществляться посредством локальной политики безопасности.

Каждый из рассматриваемых режимов функционирования операционной системы Microsoft® Windows® XP Professional предусматривает две сертифицированные конфигурации безопасности:

- «Enterprise» (Корпоративная);
- «High Security» (Высокая безопасность).

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

### **Конфигурация «Enterprise»**

Данная конфигурация подразумевает наличие инфраструктуры домена Active Directory. Управление клиентами в данной среде происходит через использование групповой политики, предоставляющей механизм централизованного управления политиками безопасности для среды функционирования в целом. Применение групповой политики осуществляется на различных уровнях иерархии Active Directory (домены, организационные подразделения), что позволяет определять как общие для всех пользователей и компьютеров домена, так и специфичные для конкретной конфигурации, параметры безопасности.

### **Конфигурация «High Security»**

Конфигурация «High Security» подразумевает наличие более ограничивающей политики безопасности и усиленные настройки безопасности для клиентских компьютеров под управлением операционной системы Microsoft® Windows® XP Professional по сравнению с конфигурацией «Enterprise». При применении данных настроек функциональность пользователя ограничивается полномочиями на выполнение только необходимых задач.

Исходя из рассмотренных режимов функционирования и конфигураций безопасности можно выделить шесть вариантов функционирования операционной системы Microsoft® Windows® XP Professional (см. таблицу 1.1).

Таблица 1.1 – Варианты функционирования операционной системы Microsoft® Windows® XP Professional

№ п/п	Варианты функционирования операционной системы
<b>Варианты функционирования операционной системы Microsoft® Windows® XP Professional при включении компьютера в домен Active Directory</b>	
1.	Клиентский компьютер в конфигурации «High Security», являющийся членом домена Active Directory.
2.	Клиентский компьютер в конфигурации «Enterprise», являющийся членом домена Active Directory.
<b>Варианты функционирования операционной системы Microsoft® Windows® XP Professional, когда компьютер не входит в домен Active Directory или является членом домена Microsoft Windows NT® 4.0 (конфигурация Stand-Alone)</b>	
3.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене на базе Active Directory.
4.	Автономный компьютер в конфигурации «High Security», функционирующий в домене на базе Active Directory.

№ п/п	Варианты функционирования операционной системы
5.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене Windows NT 4.0 (или полностью автономно).
6.	Автономный компьютер в конфигурации «High Security», функционирующий в домене Windows NT 4.0 (или полностью автономно).

## **2 Последовательность действий по настройке сертифицированной версии операционной системы Microsoft® Windows® XP Professional**

### **2.1 Общие указания по настройке параметров безопасности сертифицированной версии операционной системы Microsoft® Windows® XP Professional**

Операционная система Microsoft® Windows® XP Professional сертифицирована в конфигурациях «Enterprise» и «High Security» для шести вариантов функционирования, перечисленных в таблице 1.1.

Для реализации политики безопасности, соответствующей конфигурациям, администратор эксплуатирующей организации может настроить параметры безопасности (см. Приложение А) самостоятельно, либо (что является более предпочтительным) использовать predetermined значения параметров безопасности, представленные в файлах шаблонов безопасности сертифицированной версии операционной системы Microsoft® Windows® XP Professional. (Актуальные шаблоны безопасности можно загрузить с Центра сертифицированных обновлений по адресу <https://update.altx-soft.ru>).

Использование шаблонов безопасности позволяет упростить выполнение задач администрирования, так как единую конфигурацию безопасности можно настроить сразу для нескольких клиентских компьютеров.

**Внимание!** Перед настройкой параметров безопасности рекомендуется создать «точку восстановления», через приложение «Восстановление системы».

По умолчанию, на компьютерах под управлением операционной системы Microsoft® Windows® XP Professional для хранения шаблонов безопасности используется папка %SystemRoot%\security\templates. Эта папка не реплицируется между контроллерами домена. Таким образом, во избежание возникновения проблем с управлением версиями шаблонов безопасности, необходимо определить контроллер домена для хранения оригинала шаблонов. Оптимальной является практика, когда изменения всегда вносятся в одну и ту же копию шаблонов. Копию шаблонов безопасности необходимо хранить в защищенном от несанкционированного доступа месте, доступ к которому предоставляется только администраторам.

Настройку параметров безопасности клиентского компьютера под управлением операционной системы Microsoft® Windows® XP Professional, являющегося членом домена Active Directory, в соответствии с конфигурациями «High Security» или «Enterprise» (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 конфигурацию безопасности, описанную с помощью соответствующих шаблонов безопасности.

Альтернативой централизованному применению групповой политики является настройка каждого компьютера вручную. Рекомендованные для каждой конфигурации значения параметров (см. Приложение А) позволят обеспечить безопасность компьютеров под управлением операционной системы Microsoft® Windows® XP Professional в условиях отсутствия доменной структуры на базе службы каталогов Active Directory, создать среду, защищенную от большинства современных угроз безопасности, в которой пользователи могут продолжить эффективную работу на своих компьютерах.

Таким образом, в зависимости от режимов функционирования (в автономном режиме или в составе домена Active Directory) шаблоны безопасности необходимо применять либо непосредственно на рабочих станциях, либо на контроллере домена.

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

Таблица 2.1 – Соответствие вариантов функционирования операционной системы Microsoft® Windows® XP Professional и применяемых шаблонов безопасности

<b>№ п/п</b>	<b>Варианты функционирования операционной системы</b>	<b>Шаблоны безопасности</b>
1.	Клиентский компьютер в конфигурации «High Security», являющийся членом домена Active Directory.	XPG-SSLF-Domain.inf
		XPG-SSLF-Desktop.inf
2.	Клиентский компьютер в конфигурации «Enterprise», являющийся членом домена Active Directory.	XPG-EC-Domain.inf
		XPG-EC-Desktop.inf
3.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене на базе Active Directory.	XPG-EC-Domain.inf
		XPG-EC-Desktop.inf
4.	Автономный компьютер в конфигурации «High Security», функционирующий в домене на базе Active Directory.	XPG-SSLF-Domain.inf
		XPG-SSLF-Desktop.inf
5.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене Windows NT 4.0 (или полностью автономно).	XPG-EC-Domain.inf
		XPG-EC-Desktop.inf
6.	Автономный компьютер в конфигурации «High Security», функционирующий в домене Windows NT 4.0 (или полностью автономно).	XPG-SSLF-Domain.inf
		XPG-SSLF-Desktop.inf



### 2.2.1 Настройка клиентского компьютера, являющегося членом домена Active Directory в конфигурации «High Security» или «Enterprise»

Используемые шаблоны безопасности

Для автоматической настройки параметров политики учетных записей следует импортировать шаблоны безопасности XPG-SSLF-Domain.inf или XPG-EC-Domain.inf в объект групповой политики «Default Domain Policy» (Политика домена, используемая по умолчанию) на контроллере домена под управлением операционной системы Microsoft® Windows® 2000 Server, Microsoft® Windows Server 2003 или Microsoft® Windows Server 2008.

Для автоматической настройки параметров политики безопасности для клиентских компьютеров, являющихся членами домена Active Directory, следует импортировать шаблоны безопасности XPG-SSLF-Desktop.inf или XPG-EC-Desktop.inf в объект групповой политики на уровне организационного подразделения, содержащего учетные записи компьютеров под управлением операционной системы Microsoft® Windows® XP Professional, которые должны быть настроены.

#### Порядок применения шаблонов безопасности

Импорт шаблонов безопасности XPG-SSLF-Domain.inf или XPG-EC-Domain.inf необходимо осуществлять с использованием редактора объекта групповой политики «Default Domain Policy». Чтобы импортировать шаблон безопасности в соответствующий объект групповой политики необходимо выполнить следующие действия:

1. Вызвать редактор объектов групповой политики (Group Policy Object Editor). Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Выполнить...», в поле «Открыть» диалогового окна «Запуск программы» набрать команду «mmc» (без кавычек) и нажать «ОК» (см. рисунок 2.1).

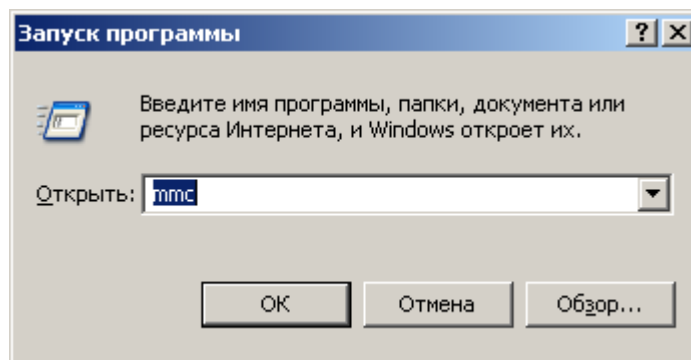


Рисунок 2.1.

В окне консоли управления MMC (MMC – Microsoft Management Console) через пункт меню «Добавить или удалить оснастку» добавить оснастку «Групповая политика» и выбрать объект групповой политики «Default Domain Policy» (см. рисунок 2.2-2.3).

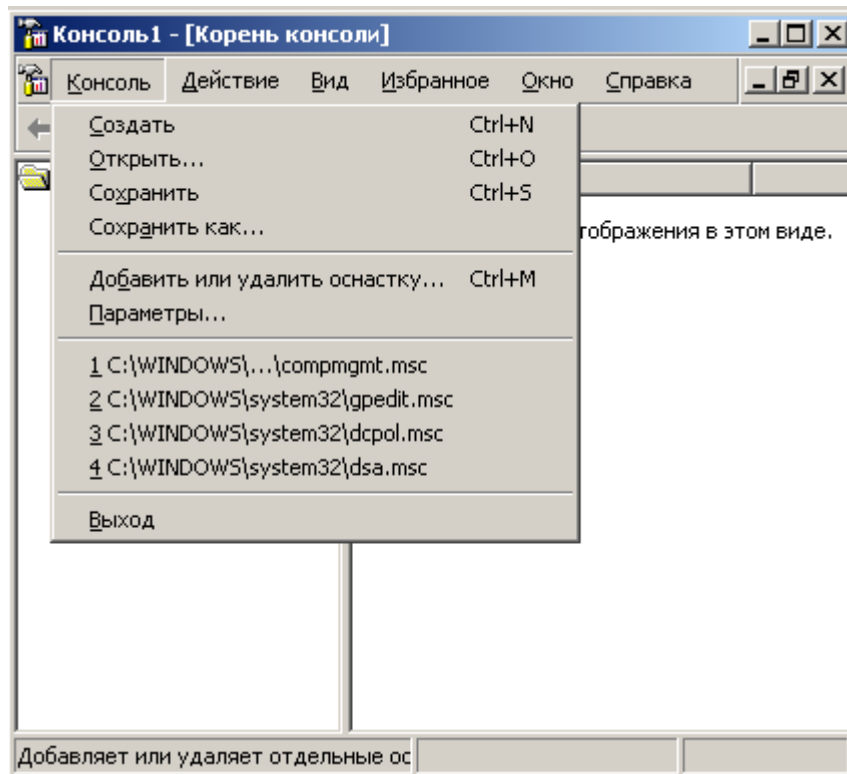


Рисунок 2.2

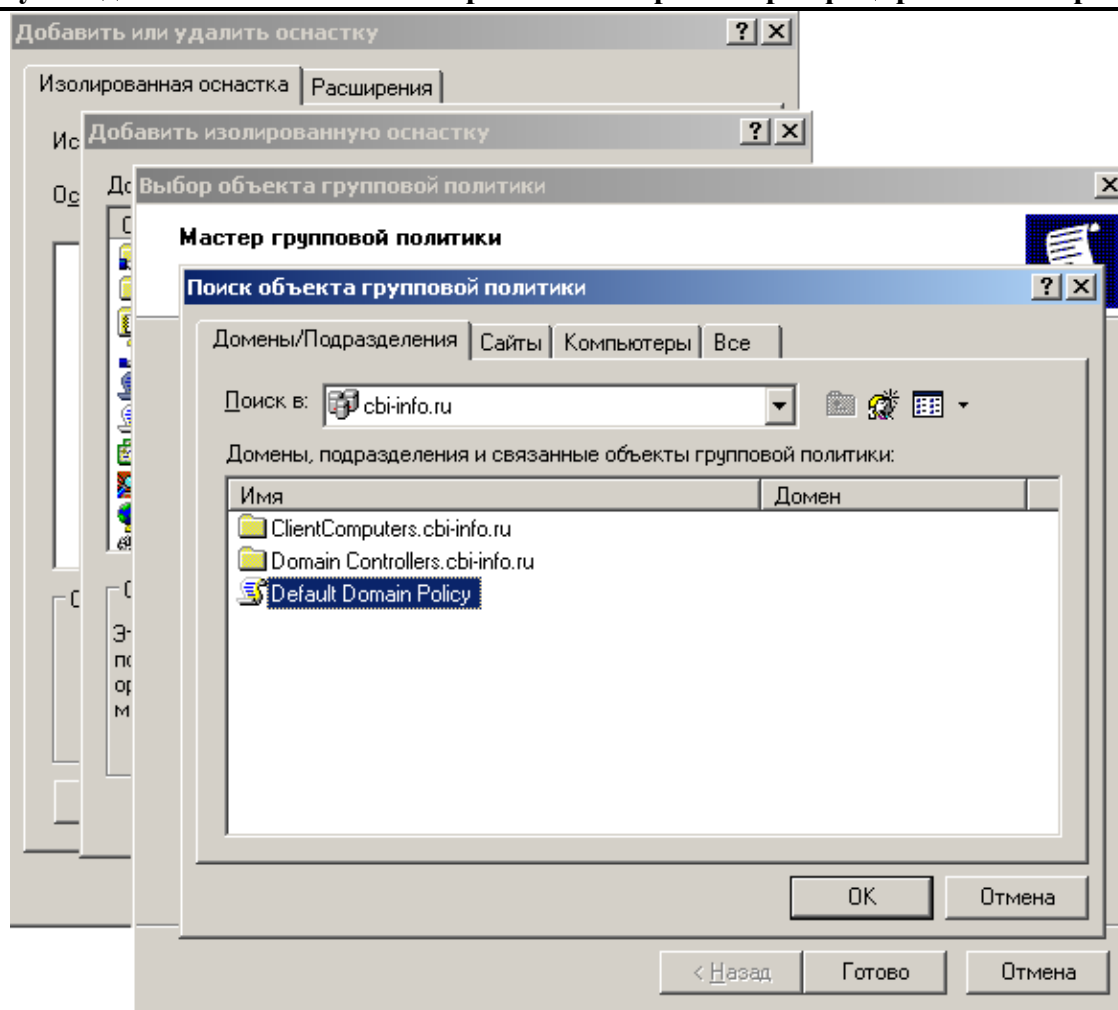


Рисунок 2.3

2. В окне редактора объектов групповой политики выбрать узел «Конфигурация компьютера» и перейти к разделу «Конфигурация Windows».
3. Выделить папку «Параметры безопасности».
4. Посредством контекстного меню выбрать пункт «Импорт политики» (см. рисунок 2.4).

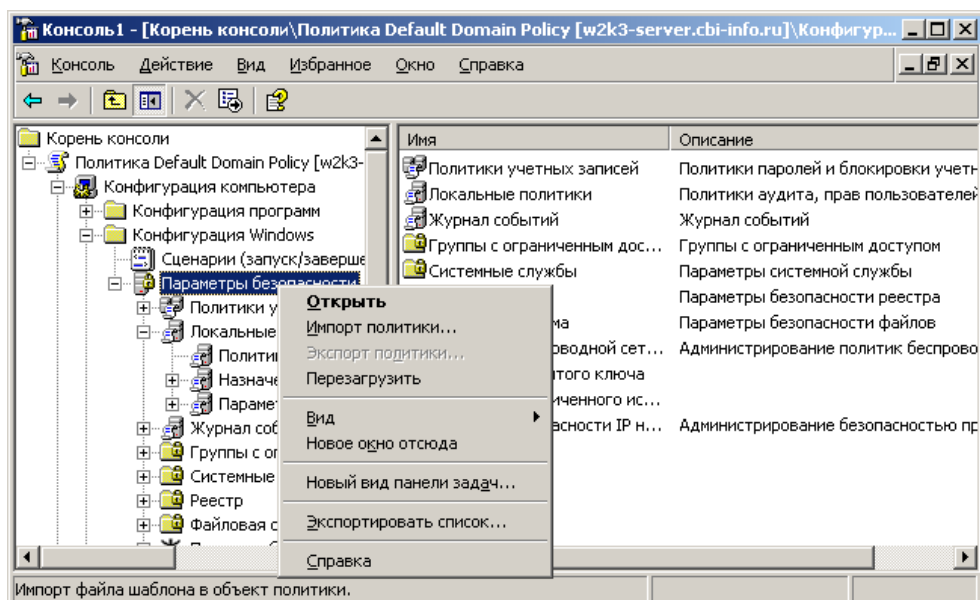


Рисунок 2.4

5. В появившемся диалоговом окне импорта политики выбрать шаблон безопасности XPG-SSLF-Domain.inf или XPG-EC-Domain.inf и нажать кнопку «Открыть». После чего параметры безопасности импортируются из выбранного файла в текущий объект групповой политики.

6. Закрыть редактор групповой политики.

При назначении политики учетных записей на уровне домена необходимо убедиться, что в списке управления доступом ACL объекта групповой политики «Default Domain Policy» 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 применена не будет. Кроме того, для групповой политики должен быть применен параметр принудительного наследования (No override) «Не перекрывать: другие объекты групповой политики не могут перекрывать параметры этой политики».

Импорт шаблонов безопасности XPG-SSLF-Desktop.inf или XPG-EC-Desktop.inf необходимо осуществлять с использованием редактора объекта групповой политики, применяемой на уровне организационного подразделения. Чтобы импортировать шаблон безопасности в соответствующий объект групповой политики необходимо выполнить следующие действия:

1. Вызвать редактор объектов групповой политики (Group Policy Object Editor). Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Выполнить...», в поле «Открыть» диалогового окна «Запуск программы» набрать команду «mmc» (без кавычек) и нажать «ОК». В окне консоли управления MMC (MMC – Microsoft Management Console) добавить оснастку «Групповая политика» и выбрать соответствующий объект групповой политики.

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

3. Выделить папку «Параметры безопасности».

4. Посредством контекстного меню выбрать пункт «Импорт политики».

5. В появившемся диалоговом окне импорта политики выбрать шаблон безопасности XPG-SSLF-Desktop.inf или XPG-EC-Desktop.inf и нажать кнопку «Открыть». После чего параметры безопасности импортируются из выбранного файла в текущий объект групповой политики.

6. Закрыть редактор групповой политики.

При назначении групповой политики на уровне организационного подразделения необходимо убедиться, что в списке управления доступом ACL данной политики разрешения «Чтение» и «Применение групповой политики» определены только для требуемой группы клиентских компьютеров.

В случае, если на уровне организационного подразделения групповая политика не определена, необходимо создать новый объект групповой политики и привязать его к соответствующему организационному подразделению. Для этого на контроллере домена вызвать оснастку «Active Directory – пользователи и компьютеры». Перейти в окне свойств соответствующего организационного подразделения на вкладку «Групповая политика» и нажать кнопку «Создать». Ввести имя нового объекта групповой политики (см. рисунок 2.5).

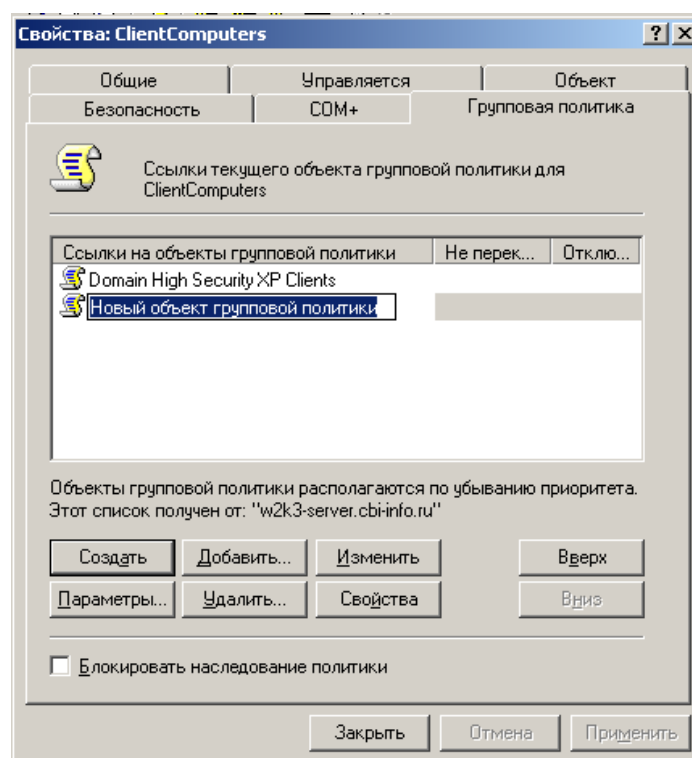


Рисунок 2.5

### **2.2.2 Настройка автономного компьютера в конфигурации «High Security» или «Enterprise», функционирующего в домене Active Directory, Windows NT 4.0 или полностью автономно.**

Используемые шаблоны безопасности

С целью обеспечения требуемого уровня безопасности, необходимого для обработки конфиденциальной информации, автономные компьютеры под управление операционной системы Microsoft® Windows® XP Professional в конфигурации «High Security» или «Enterprise», должны использоваться параметры безопасности, определенные в соответствующих шаблонах (Таблица 2.1).

Для настройки политики учетных записей и параметров безопасности для автономного компьютера в конфигурации «High Security» или «Enterprise» импорт шаблонов безопасности должен осуществляться на уровне локальной политики безопасности.

### **Порядок применения шаблонов безопасности**

Импорт шаблонов безопасности можно осуществлять с использованием графического интерфейса Windows (оснастки «Анализ и настройка безопасности»).

Чтобы импортировать шаблоны безопасности необходимо выполнить следующие действия:

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

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» и выполнить одно из следующих действий (см. рисунок 2.6):

- чтобы создать новую базу данных, необходимо ввести новое имя в поле «Имя файла» и нажать кнопку «Открыть». При открытии новой базы данных в диалоговом окне «Импорт шаблона» выбрать один из импортируемых шаблонов безопасности и нажать кнопку «Открыть»;
- чтобы открыть существующую базу данных, необходимо выбрать базу данных и нажать кнопку «Открыть».

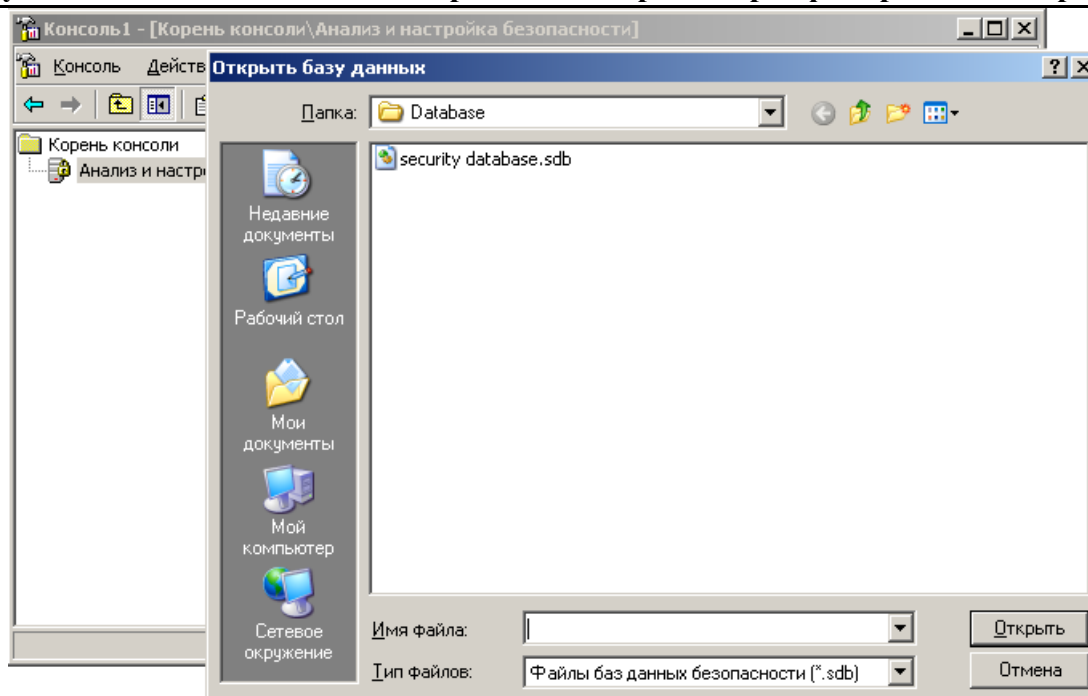


Рисунок 2.6

4. Последовательно импортировать соответствующие шаблоны безопасности (Таблица 2.1), определяющие параметры политики учетных записей и параметры политики безопасности:

- в случае использования существующей базы данных и последующим импортированием 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 этот флажок снят, импортированный шаблон будет объединен с сохраненными шаблонами, и в базе данных будет храниться составной шаблон безопасности. Данный вариант следует выбрать при импорте оставшегося шаблона безопасности, используемого для настройки безопасности системы;
- в случае использования новой базы данных необходимо импортировать оставшийся шаблон безопасности, определенный для данной конфигурации. При этом необходимо убедиться, что флажок «Очистить эту базу данных перед импортом» снят.

5. Посредством нажатия правой кнопкой мыши узла «Анализ и настройка безопасности» выбрать команду «Настроить компьютер» (см. рисунок 2.7).

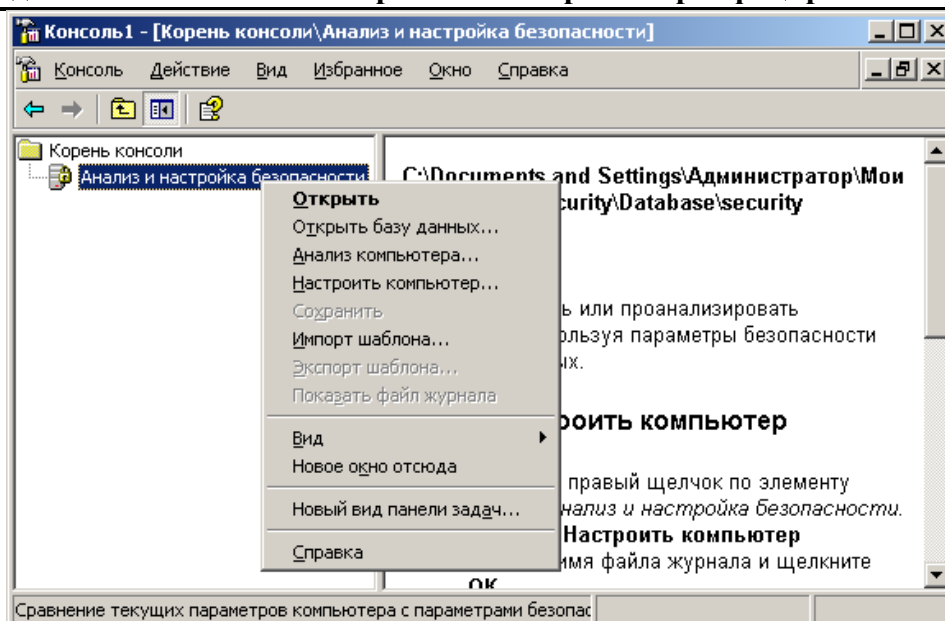


Рисунок 2.7

6. Закрыть оснастку «Анализ и настройка безопасности».
7. Для вступления настроек в силу может потребоваться перезагрузка компьютера.

### 2.3 Порядок отключения функции автоматического обновления операционной системы Microsoft® Windows® XP Professional

Одним из основных условий соответствия сертифицированной версии ОС Microsoft® Windows® XP Professional 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 (Service Pack), доступных на защищенном разделе сайта «<http://check.altx-soft.ru/>», необходимо отключить функцию автоматического обновления операционной системы Microsoft® Windows® XP Professional . В результате пользователь не будет получать уведомления о доступных обновлениях и приглашения на их загрузку и установку.

Для отключения функции автоматического обновления операционной системы Microsoft® Windows® XP Professional необходимо выполнить следующие действия:

1. Отключить компонент «Автоматическое обновление»:
  - осуществить вход в систему с использованием учетной записи администратора;
  - нажать кнопку «Пуск», выбрать пункт «Панель управления» и далее «Система»;



- перейти на вкладку «Автоматическое обновление»;
- выбрать опцию «Отключить автоматическое обновление» (см. рисунок 2.17).

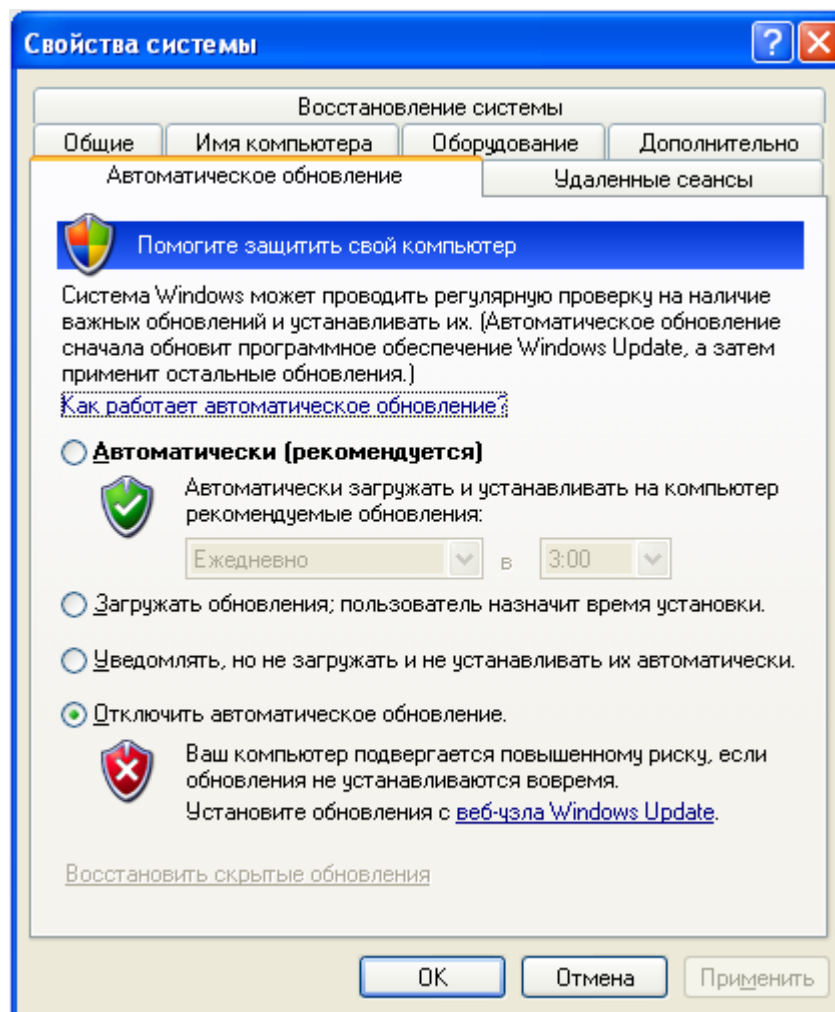


Рисунок 2.17

- 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», выбрать пункт «Панель управления» и далее «Производительность и обслуживание»;
  - в диалоговом окне «Производительность и обслуживание» 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 2.18);

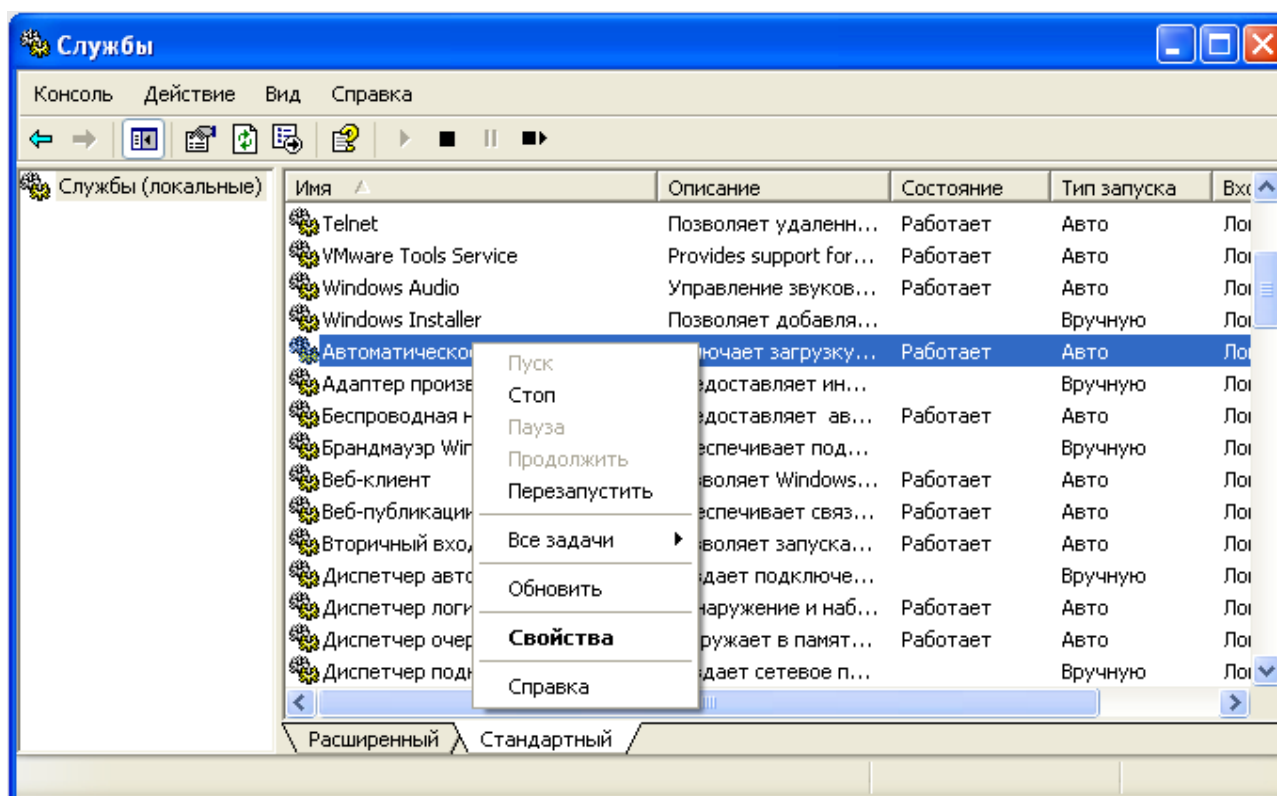


Рисунок 2.18

- в окне свойств службы «Автоматическое обновление» изменить тип запуска на «Отключено» и посредством нажатия кнопки «Стоп» остановить службу (см. рисунок 2.19);

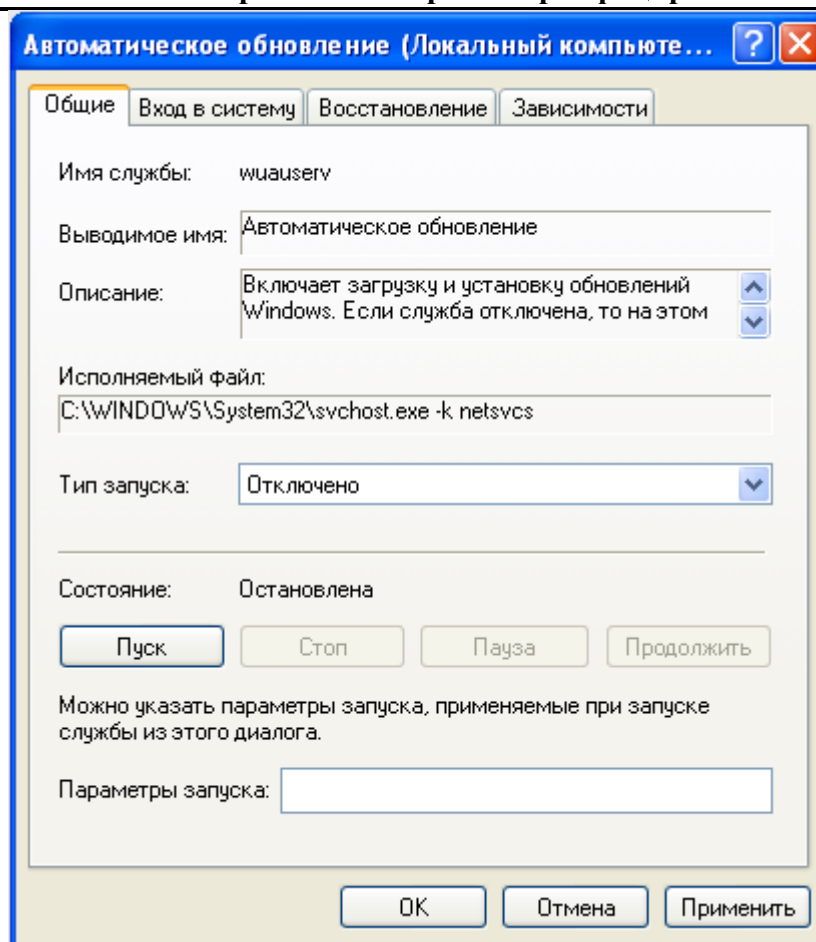


Рисунок 2.19

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

Кроме того, отключение функции автоматического обновления операционной системы Microsoft® Windows® XP Professional 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» (без кавычек) и нажать «ОК»;
- в окне редактора 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 Wuaui.adm, расположенный в папке %SystemRoot%\Inf, и нажать кнопку «Открыть» (см. рисунок 2.20);

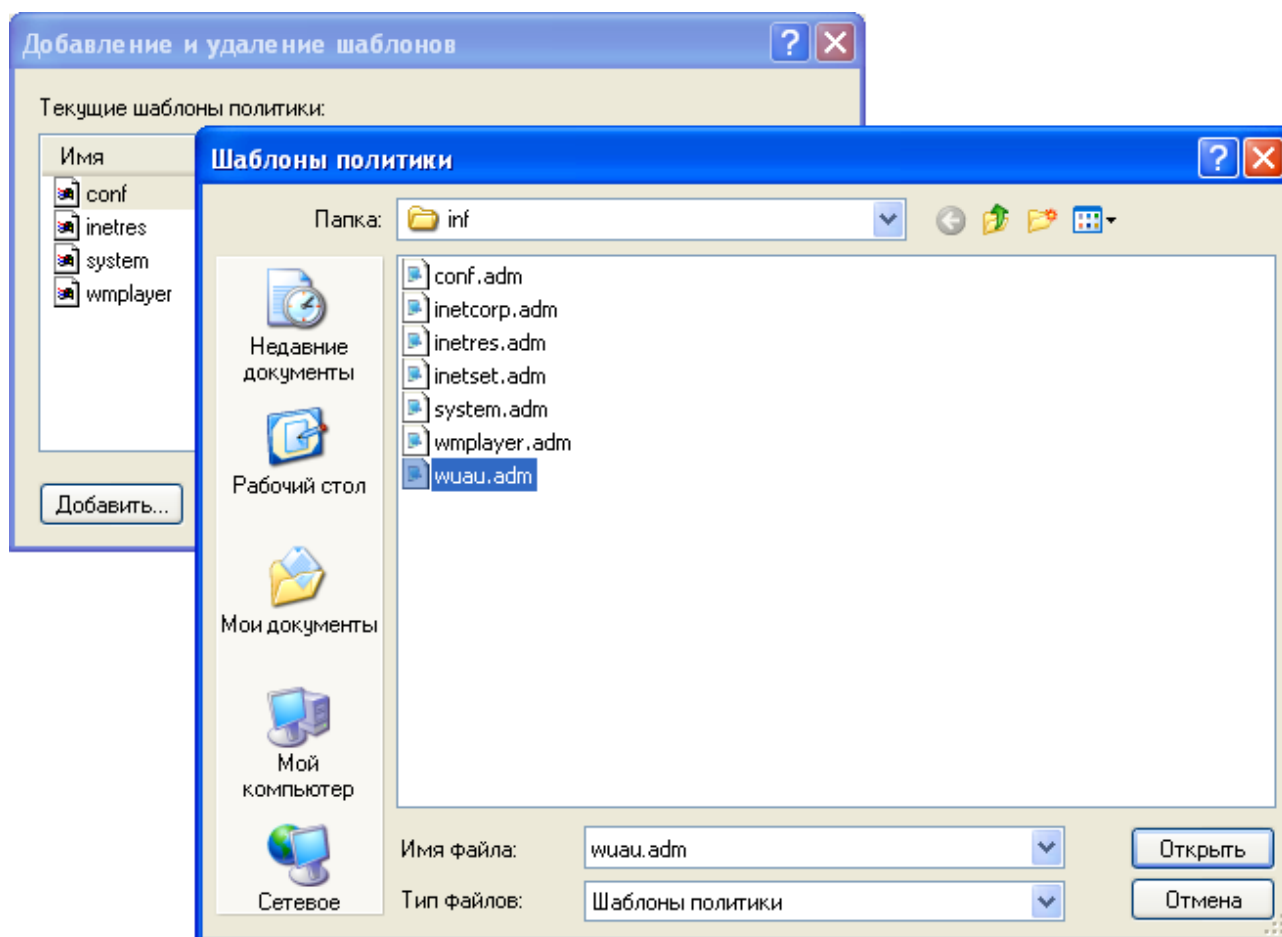


Рисунок 2.20

- нажать кнопку «Заккрыть»;
- в дереве «Конфигурация компьютера» последовательно развернуть узлы «Административные шаблоны», «Компоненты Windows» и «Windows Update». В результате появится политика «Настройка автоматического обновления», в которой указано, использует ли клиентский компьютер службу автоматического обновления операционной системы Microsoft® Windows® XP Professional для получения обновлений безопасности и других исправлений. Параметры данной политики предназначены для настройки службы автоматического обновления операционной системы;

- выбрать параметр политики «Настройка автоматического обновления» и посредством двойного нажатия открыть диалоговое окно его свойств;
- на вкладке «Параметр» выбрать опцию «Отключен» (см. рисунок 2.21);

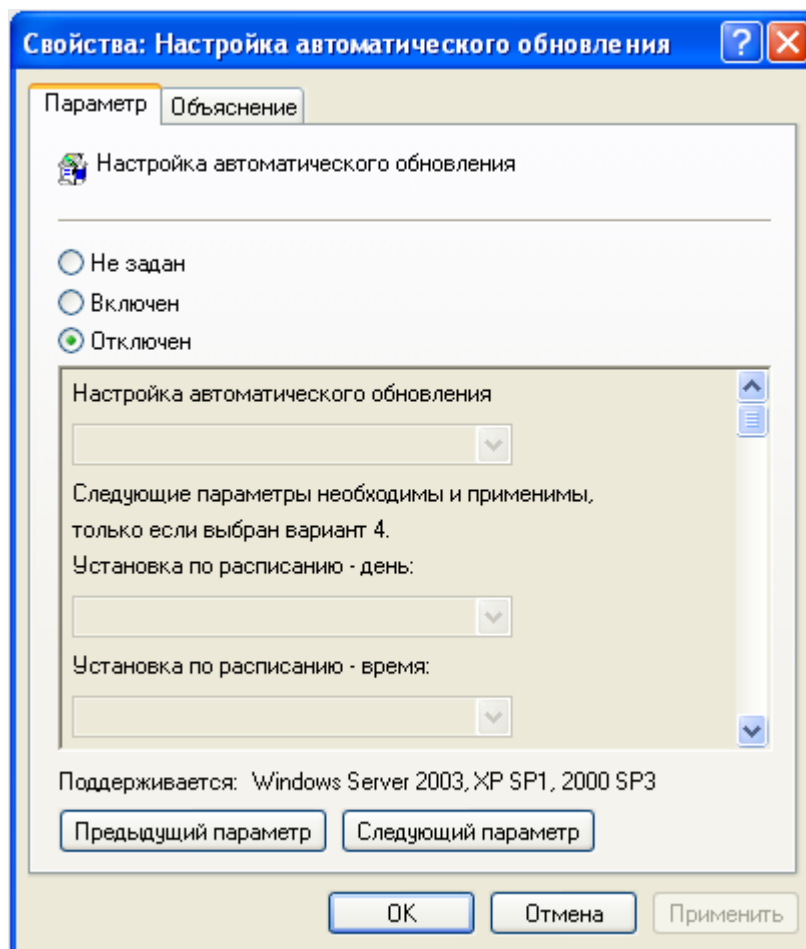


Рисунок 2.21

- закрыть редактор объекта групповой политики;
- посредством команды `gpupdate /force` осуществить обновление параметров групповой политики.

Для отключения компонента «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;
- нажать кнопку «Пуск» и выбрать пункт «Выполнить...»;
- в поле «Открыть» диалогового окна «Запуск программы» набрать команду «`dsa.msc`» (без кавычек) и нажать «OK»;

- 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 объект групповой политики и нажать кнопку «Изменить» (в случае создания нового объекта групповой политики необходимо выбрать кнопку «Создать», ввести имя политики и нажать кнопку «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 кнопку «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;
- осуществить обновление параметров групповой политики.

### **Управление параметрами оповещения «Центра обеспечения безопасности»**

При отключении функции автоматического обновления «Центром обеспечения безопасности», осуществляющим постоянный мониторинг уровня безопасности компьютера, включая состояние брандмауэра, параметры автоматического обновления и защиту от вирусов, периодически будут выводиться оповещения, свидетельствующие, что параметры автоматического обновления не удовлетворяют требованиям безопасности компьютера. Чтобы исключить вывод «Центром обеспечения безопасности» данных оповещений, администратором необходимо выполнить настройку параметров оповещений «Центра обеспечения информации»:

1. Через панель управления осуществить вызов консоли управления «Центр обеспечения безопасности».
2. В левой части диалогового окна консоли управления в разделе «Ресурсы» выбрать пункт «Изменить способ оповещений Центром обеспечения безопасности».

3. В появившемся диалоговом окне «Параметры оповещений» снять опцию «Автоматическое обновление» (см. рисунок 2.22).

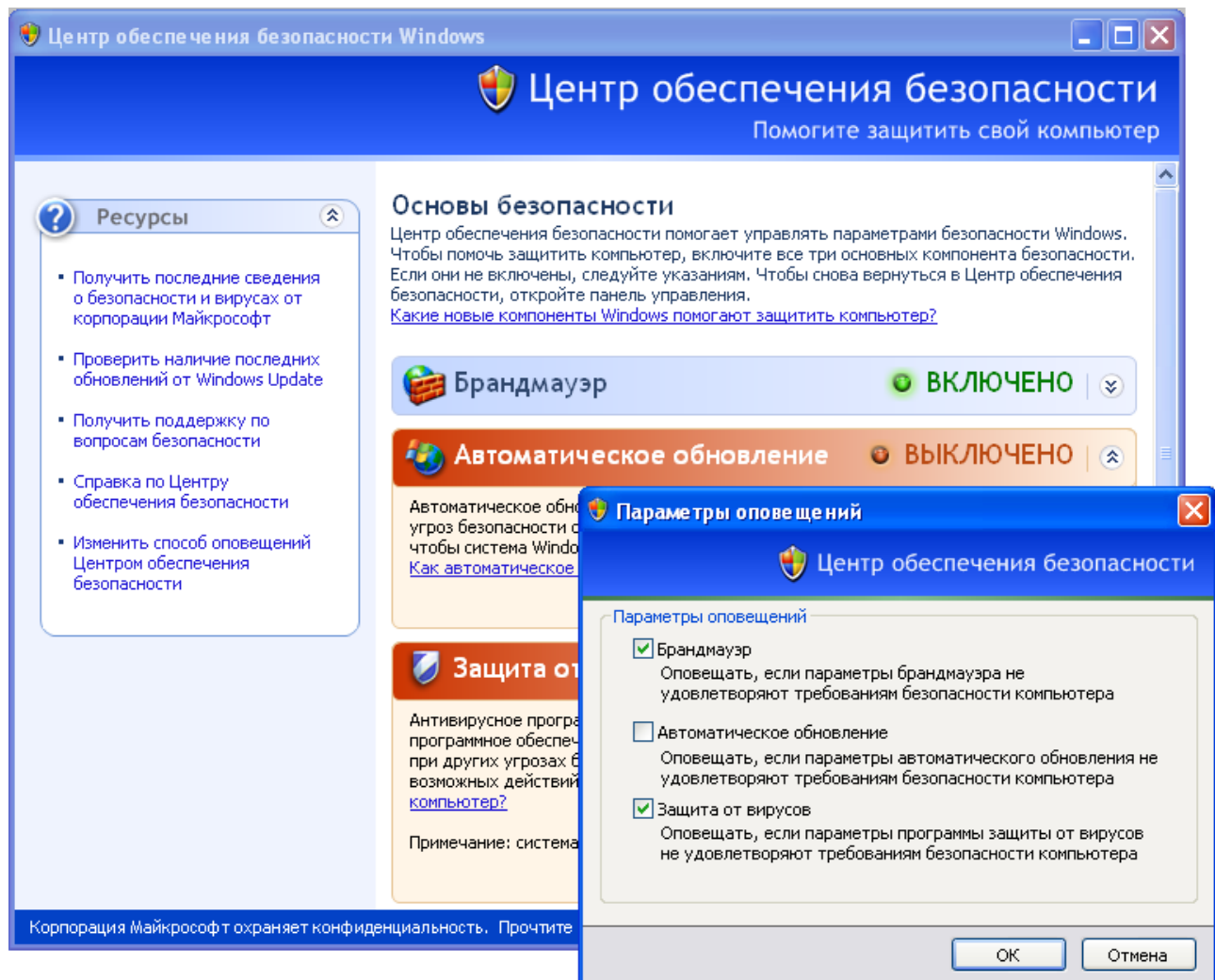


Рисунок 2.22

## 2.4 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 клиентских компьютеров под управлением операционной системы Microsoft® Windows® XP Professional рекомендованной к использованию в конфигурации «High Security», необходимо отключить эту функцию, в политике безопасности. Использование данной политики позволит отключить кнопку «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® XP Professional функционирует на клиентском компьютере, который не входит в состав домена Active Directory или является членом домена Microsoft Windows NT® 4.0 (или полностью автономным) параметры безопасности должны определяться для каждого компьютера вручную через локальную политику безопасности. В случае, если операционная система Microsoft® Windows® XP Professional функционирует на клиентском 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 (Group Policy Object Editor). Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Выполнить...», в поле «Открыть» диалогового окна «Запуск программы» набрать команду «mmc» (без кавычек) и нажать «ОК».
2. В окне консоли управления MMC (MMC – Microsoft Management Console) через пункт меню «Добавить или удалить оснастку» добавить оснастку «Групповая политика» и выбрать соответствующий объект групповой политики.
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 2.23).



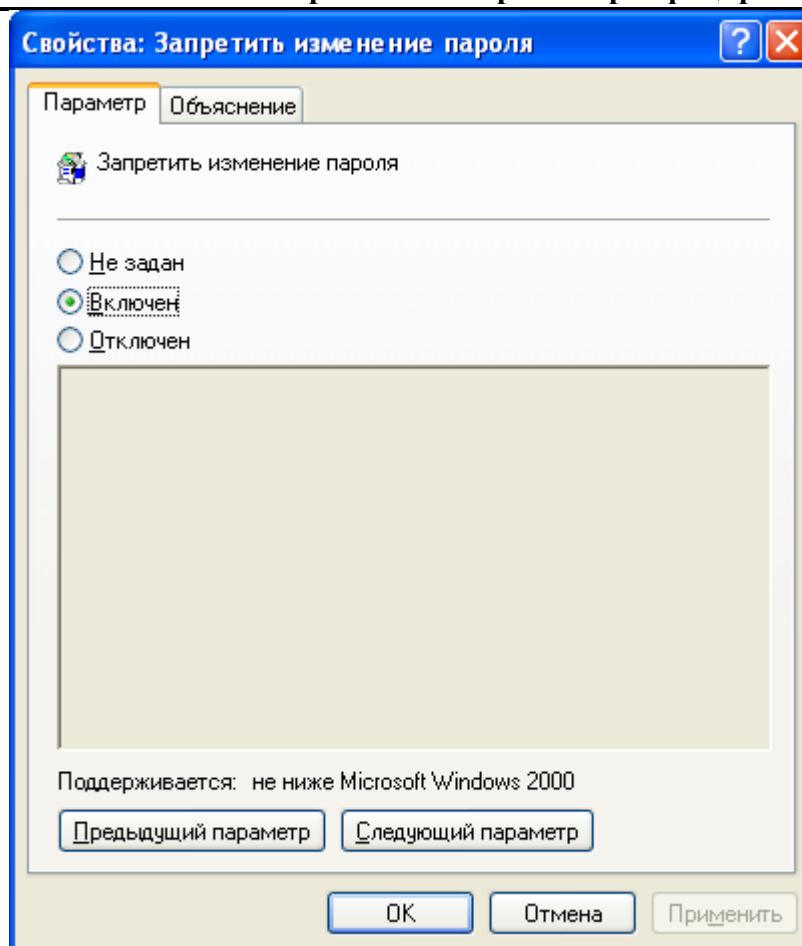


Рисунок 2.23

6. Закрывать редактор объектов групповой политики.
7. Посредством команды `gpupdate /target:user /force` осуществить обновление параметров групповой политики.

## 2.5 Настройка рекомендуемых параметров безопасности брандмауэра Windows

С целью обеспечения требуемого уровня безопасности, необходимого для обработки конфиденциальной информации, на клиентских компьютерах под управление операционной системы Microsoft® Windows® XP Professional с помощью «Центра обеспечения безопасности Windows» - инструментария управления параметрами безопасности, позволяющего отслеживать и оценивать существующий уровень безопасности компьютера, включая состояние брандмауэра, параметры автоматического обновления и защиту от вирусов – необходимо проконтролировать включение встроенного брандмауэра Windows, функции автоматического обновления и функции контроля над установленным антивирусным программным обеспечением.

В случае если политика безопасности организации не предусматривает применение персональных брандмауэров на компьютерах под управлением операционной системы

**Руководство по безопасной настройке и контролю сертифицированной версии**

Microsoft® Windows® XP Professional, они могут быть выключены. При этом должны быть обеспечены адекватные меры по защите клиентских компьютеров при организации взаимодействия как с внешними вычислительными сетями (например, посредством использования межсетевых экранов уровня предприятия, установленных на периметре ЛВС), так и в рамках внутренней вычислительной сети.

**Порядок настройки параметров безопасности брандмауэра Windows**

Настройку параметров безопасности брандмауэра Windows необходимо осуществлять с использованием редактора соответствующего объекта групповой политики в следующем разделе пространства имен объекта групповой политики: Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения\Брандмауэр Windows (см. рисунок 2.34).

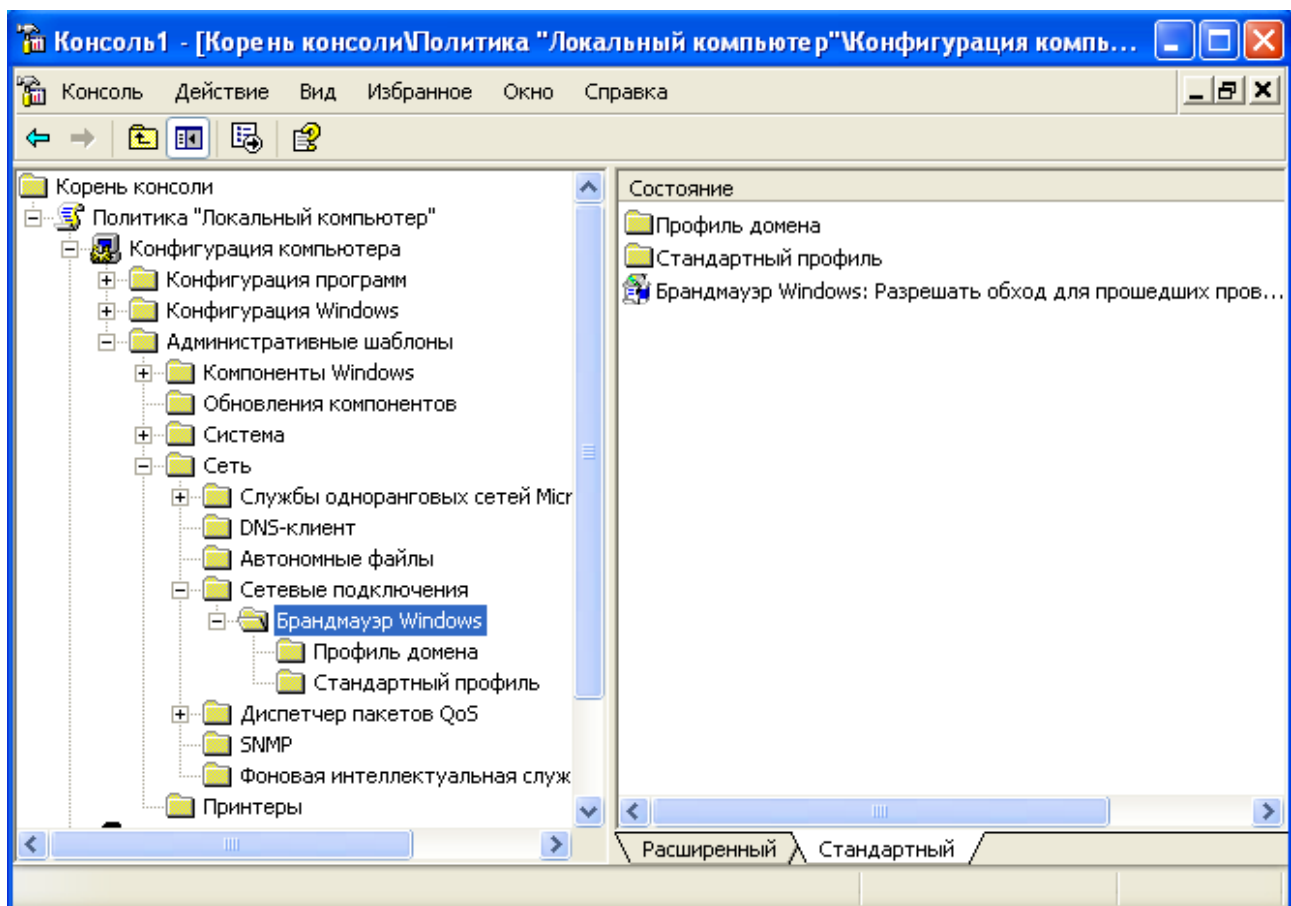


Рисунок 2.34

В случае, если операционная система Microsoft® Windows® XP Professional функционирует на клиентском компьютере, который не входит в состав домена Active Directory или является членом домена Microsoft Windows NT® 4.0 (или полностью автономным) параметры безопасности брандмауэра Windows должны определяться для каждого компьютера вручную в объекте групповой политики «Локальный компьютер» в разделе пространства имен объекта групповой политики: Конфигурация компьютера/Административные

---

шаблоны/Сеть/Сетевые подключения/ Брандмауэр Windows/Стандартный профиль.

В случае, если операционная система Microsoft® Windows® XP Professional функционирует на клиентском 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 указанных компьютеров), что позволит всем компьютерам, на которые распространяется групповая политика, автоматически применить требуемую конфигурацию безопасности. В этом случае параметры безопасности должны определяться в следующем разделе пространства имен объекта групповой политики: Конфигурации компьютера/Административные шаблоны/Сеть/Сетевые подключения/Брандмауэр Windows/Профиль домена.

Чтобы осуществить настройку рекомендованных значений параметров безопасности брандмауэра Windows необходимо выполнить следующие действия:

1. Вызвать редактор объектов групповой политики (Group Policy Object Editor). Для этого необходимо нажать кнопку «Пуск», выбрать пункт «Выполнить...», в поле «Открыть» диалогового окна «Запуск программы» набрать команду «gpedit» (без кавычек) и нажать «ОК».

2. В окне консоли управления MMC (MMC – Microsoft Management Console) через пункт меню «Добавить или удалить оснастку» добавить оснастку «Групповая политика» и выбрать соответствующий объект групповой политики (см. рисунок 2.35).

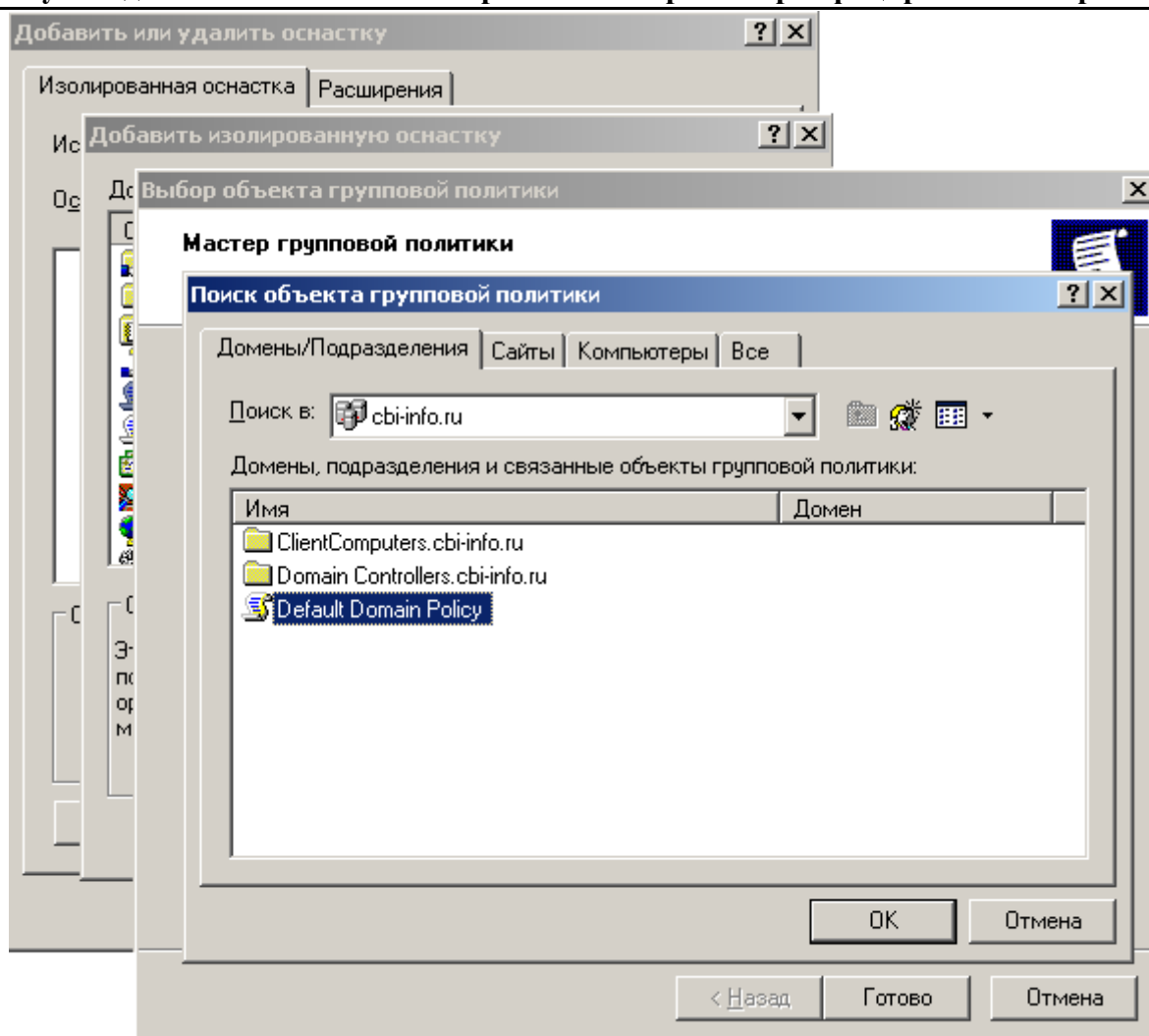


Рисунок 2.35

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

4. Выделить папку Сеть/Сетевые подключения/Брандмауэр Windows/Профиль домена или Сеть/Сетевые подключения/Брандмауэр Windows/Стандартный профиль (в зависимости от варианта функционирования операционной системы Microsoft® Windows® XP Professional ) и перейти в левую часть окна редактора объектов групповой политики.

5. Посредством двойного нажатия соответствующего параметра безопасности вызвать диалоговое окно и назначить рекомендованное для данного параметра значение (см. рисунок 2.36).

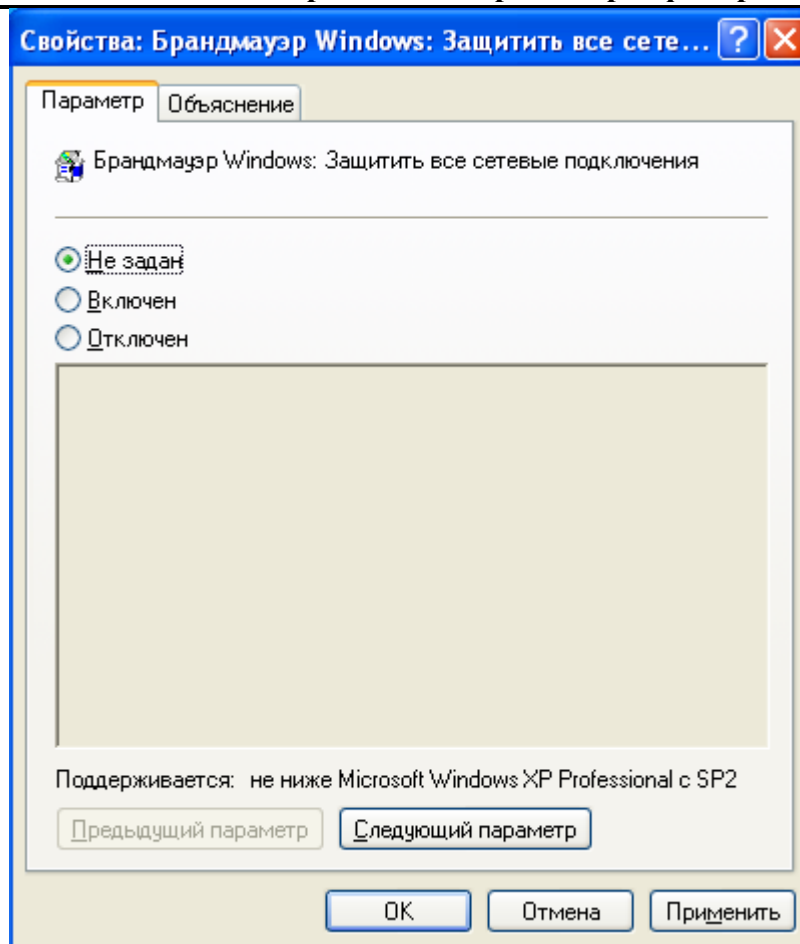


Рисунок 2.36

6. Выполнить указанную процедуру назначения рекомендованных значений для всех параметров безопасности брандмауэра Windows.
7. Закрыть редактор объектов групповой политики.
8. Посредством команды `gpupdate /force` осуществить обновление параметров групповой политики.

Детальное описание и рекомендованные для каждой конфигурации значения параметров безопасности брандмауэра Windows представлены в Приложение «В» настоящего руководства.

### 3 Последовательность действий по контролю сертифицированной версии операционной системы Microsoft® Windows® XP Professional

Контроль маркирования сертифицированной версии операционной системы «Microsoft® Windows® XP Professional» 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® XP Professional, тому ПО, которое установлено на рабочей станции.

#### 3.1 Контроль маркирования сертифицированной версии операционной системы Microsoft® Windows® XP Professional

Порядок проведения контроля маркирования:

1. Удостовериться, что комплект поставки сертифицированной версии «Microsoft® Windows® XP Professional» 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® Windows® XP Professional.

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 2.8 Формуляра на сертифицированную версию Microsoft® Windows® XP Professional.

#### 3.2 Автоматизированный контроль сертифицированной версии операционной системы Microsoft® Windows® XP Professional

Назначение программы «XP\_Check»

Для контроля сертифицированной версии операционной системы Microsoft® Windows® XP, а так же обновлений безопасности для неё, используется программа контроля сертифицированной версии ОС Microsoft® Windows® XP Professional «XP\_Check», поставляемая дополнительно к дистрибутиву ОС на компакт-диске Media Kit.

Программа «XP\_Check» предназначена для решения следующих задач:

- проверка сертифицированной версии Windows и просмотр отчета по контролю систем;
- проверка и просмотр отчета по контролю обновлений системы;
- фиксация и контроль системных файлов Windows;
- создание проекта аттестата соответствия.

Установка и запуск на выполнение программы «XP\_Check»

Для установки программы необходимо выполнить следующую последовательность действий:

1) Начать сеанс Microsoft® Windows® XP Professional 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 установлен). 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 «АЛТЭКС-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).

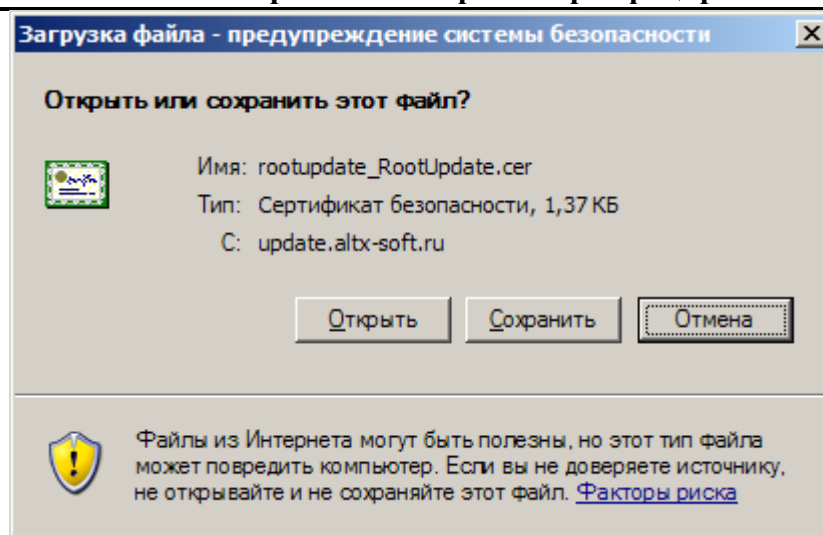


Рисунок 3.2- Открытие цифрового сертификатов удостоверяющего центра  
ЗАО «АЛТЭКС-СОФТ»

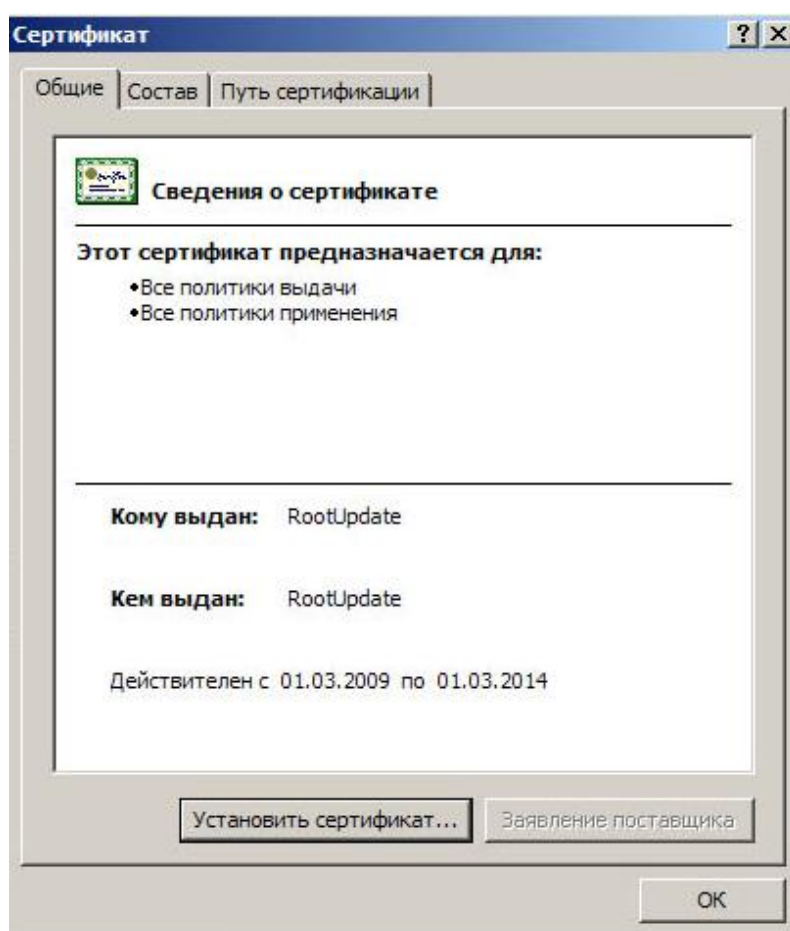


Рисунок 3.3 - Установка цифрового сертификатов удостоверяющего центра  
ЗАО «АЛТЭКС-СОФТ»

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 (см. рисунок 3.4).

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

Главное окно программы представлено на рисунке 3.5.

При каждом запуске программа «XP\_Check» выполняет контроль версии контролируемой системы, в случае если версия операционной системы не соответствует сертифицированной, на экран будет выведено сообщение, представленное на рисунке 3.6.

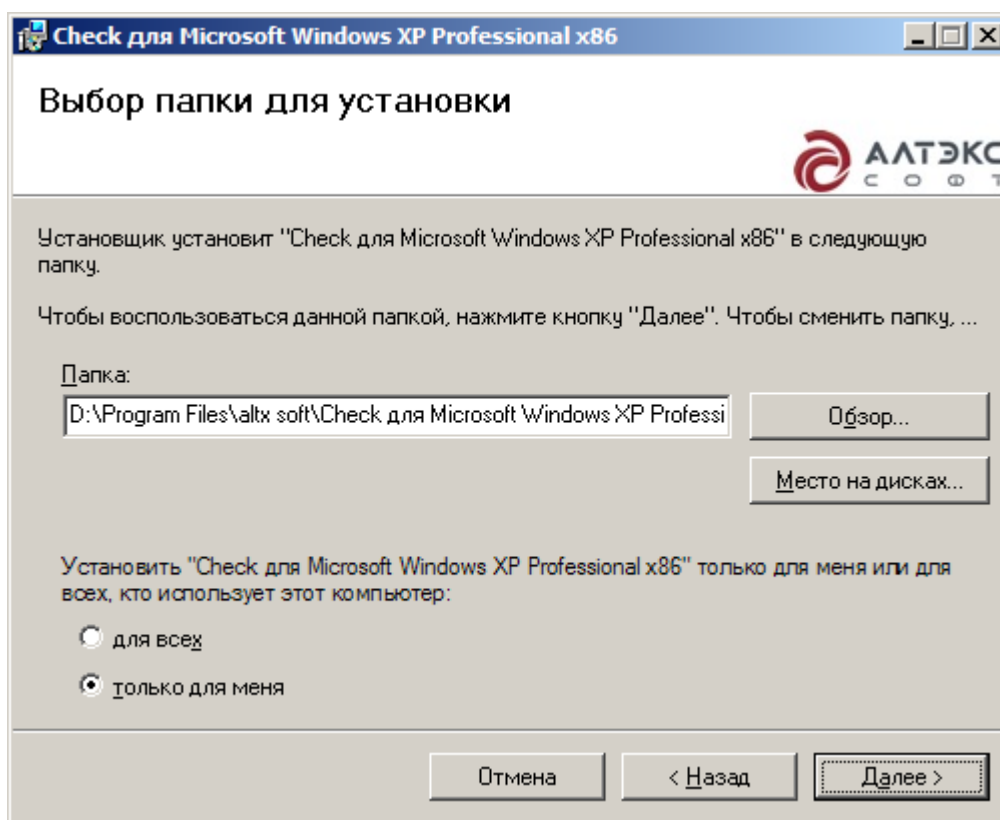


Рисунок 3.4 – Выбор каталога установки и пользователей программы «XP\_Check»

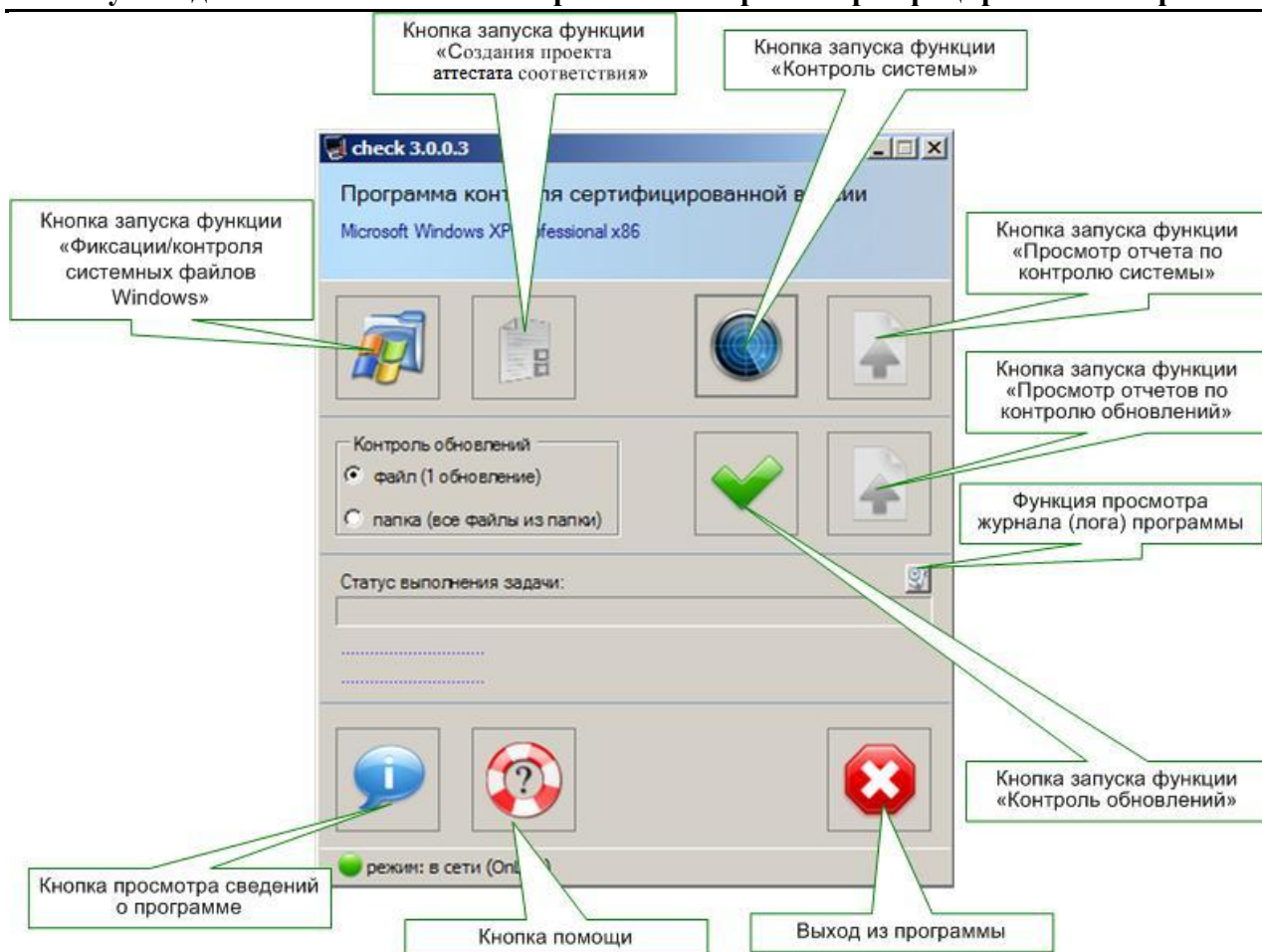


Рисунок 3.5 –Главное окно программы контроля сертифицированной версии ОС Microsoft® Windows® XP Professional «XP\_Check»

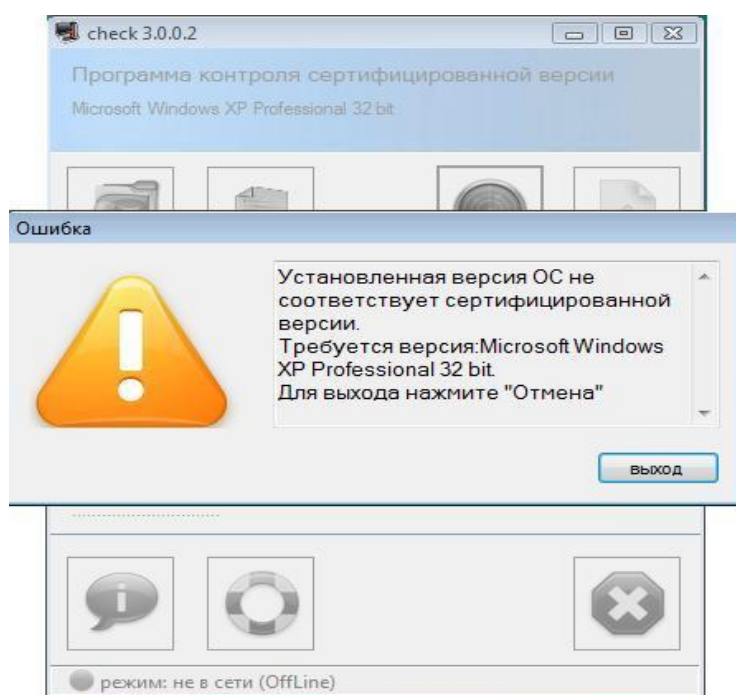



Рисунок 3.6 – Вид окна программы при несоответствии версии ОС Microsoft® Windows® XP Professional

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  режим: не в сети (OffLine). 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 3.7.

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



Рисунок 3.7 – Окно программы при отсутствии доступа в сеть Интернет

Примечание: 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 3.8.

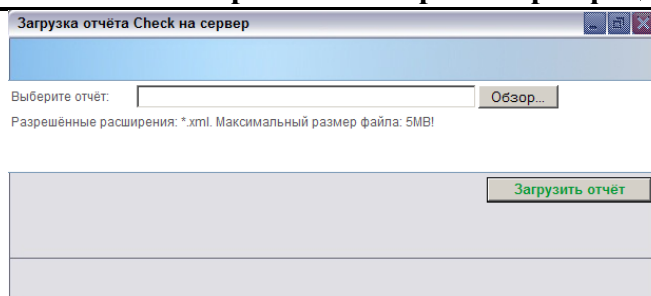




Рисунок 3.8 – Вид окна загрузки отчета программы сформированного при отсутствии подключения к сети Интернет

Выполнение программы «XP\_Check»

*Проверка сертифицированной версии Windows и просмотр отчета по контролю системы*

Чтобы произвести проверку соответствия установленной Microsoft® Windows® XP Professional сертифицированной версии необходимо нажать кнопку 

В случае корректной установки на экран будет выведено сообщение, представленное на рисунке 3.9. После проведения проверки сертифицированной версии Windows 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 завершения контроля, т.е. полного соответствия текущей версии операционной системы Microsoft® Windows® XP сертифицированной версии и установленных всех сертифицированных обновлений на экране будет отображено окно, изображенное на рисунке 3.10.

В случае соответствия текущей версии операционной системы Microsoft® Windows® XP Professional сертифицированной, но отсутствии некоторых критических для безопасности системы обновлений, патчей или Service Pack на экране пользователя будет отображено окно, изображенное на рисунке 3.11, где будут указаны необходимые для установки обновлений безопасности ссылки на сайт корпорации Microsoft.

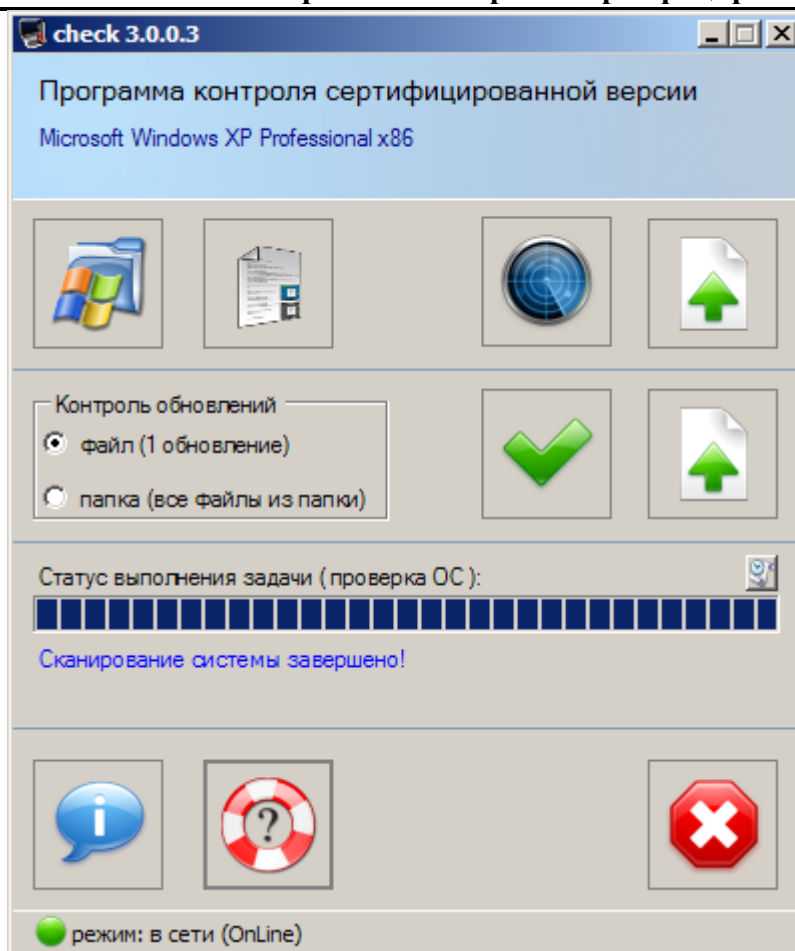


Рисунок 3.9 – Проверка сертифицированной версии Microsoft® Windows® XP Professional

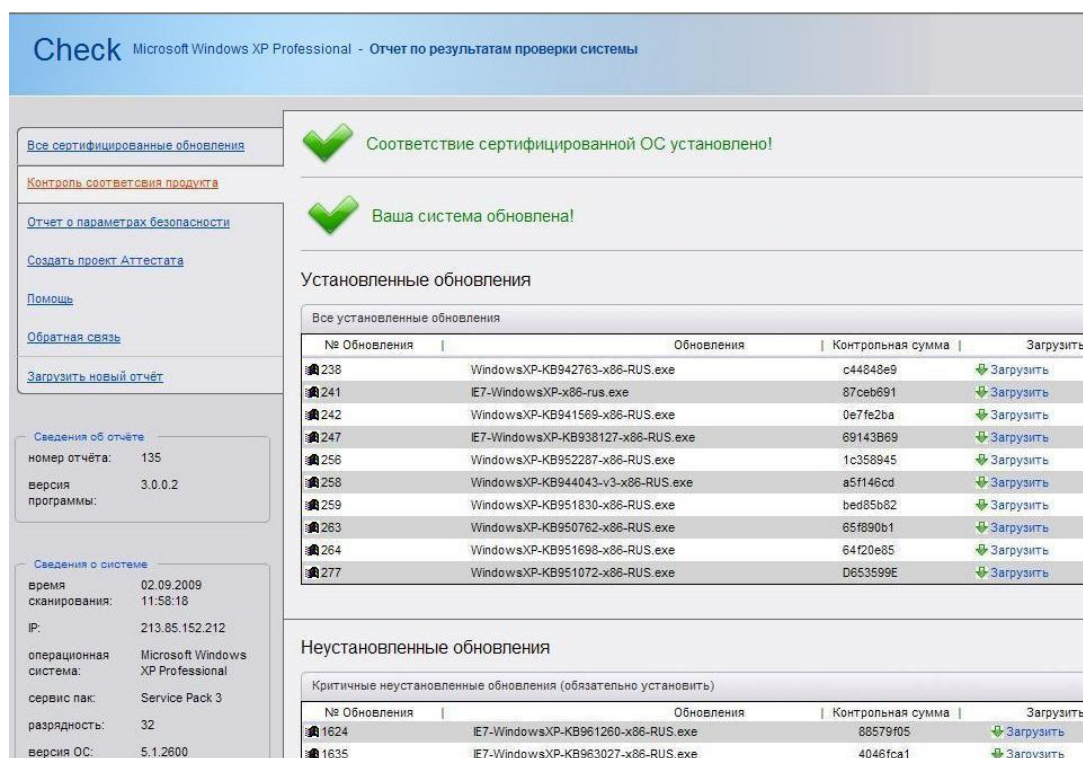


Рисунок 3.10 – Вид окна программы контроля сертифицированной версии ОС Microsoft® Windows® XP Professional при полном соответствии файлов и обновлений безопасности.



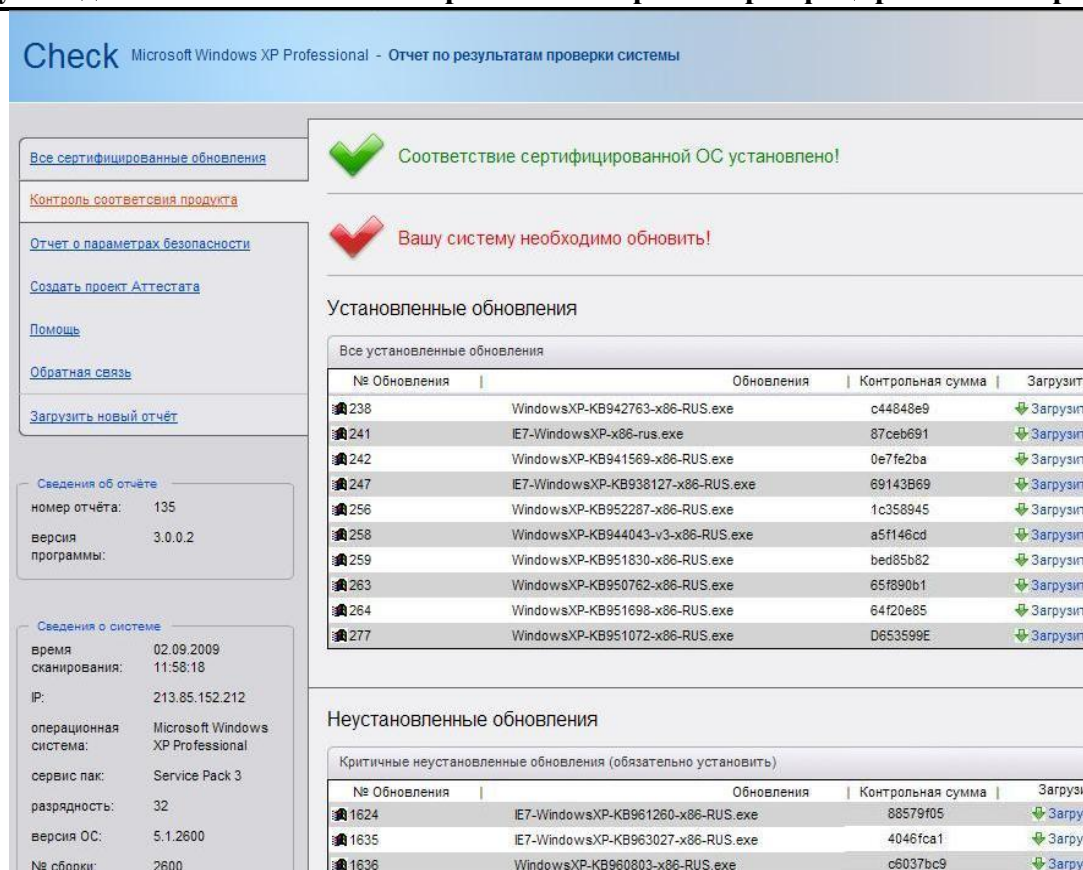




Рисунок 3.11 – Вид окна программы контроля сертифицированной версии ОС Microsoft® Windows® XP Professional при неполном соответствии обновлений безопасности.

### Проверка и просмотр отчета по контролю обновлений системы

Важной особенностью программы «XP\_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 3.12.


Результаты контроля сертификации обновлений ...				
Check — Отчет по результатам контроля обновлений Microsoft.				
файл	контрольная сумма (уровень 3)	сертифицировано	размер (байт)	путь к файлу
E7-WindowsXP-KB969897-x86-RUS.exe	5FC27CDDA24CB67DEB67220E32ECBD58AF25A92959AB8AF8F5E0912D276DA147	не определено	9236864	D:\Обновления\10.06.2009\MS Windows XP SP3\E7-WindowsXP-KB969897-x86-RUS.exe
WindowsServer2003-WindowsXP-KB963093-x86-ENU.exe	F8CB0837CC189342BE19BFC76EAC92301B0C7AF60216AF2C84F0B3BC2992DD0B	не определено	979208	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsServer2003-WindowsXP-KB963093-x86-ENU.exe
WindowsXP-KB961501-x86-RUS.exe	0A542494FFA13C7AD5F7E2E98C3815AD86AE25E6AD8031A104281A4F3950E0E3	не определено	670584	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB961501-x86-RUS.exe
WindowsXP-KB968537-x86-RUS.exe	1347AF6CF063896CF04687DA1EF6BA44C1C3344938C153884CF5332E1AF0DAF5	не определено	1474448	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB968537-x86-RUS.exe
WindowsXP-KB969897-x86-RUS.exe	D2A7626C37C9518E4DBB385FD990E1A51DA84AE2D4F716772B18905B2738E735	не определено	4963216	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB969897-x86-RUS.exe
WindowsXP-KB970238-x86-RUS.exe	A44DC64E7CD3DA3697DA057CC2342C6283DC8CF36DE752F836DF87339EA4506	не определено	868704	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB970238-x86-RUS.exe
WindowsXP-KB970437-x86-RUS.exe	DC82BBA3A5B36CC0C7151B5559888F01389FA99F8F80231A550536757C3C5	не определено	1237880	D:\Обновления\10.06.2009\MS Windows XP SP3\WindowsXP-KB970437-x86-RUS.exe
WindowsXP-KB970483-x86-RUS.exe	05BE891714230CE21E950DE95265D3E80C3C417755258FF4DF74FB1FAC11174	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 3.13).

В случае, если соответствие файлов ОС, установленной на ПЭВМ, и файлов сертифицированной ОС Microsoft® Windows® XP 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 Windows*

Операция фиксации и контроля системных файлов Windows производится при нажатии кнопки  главного окна программы (см. рисунок 3.14).

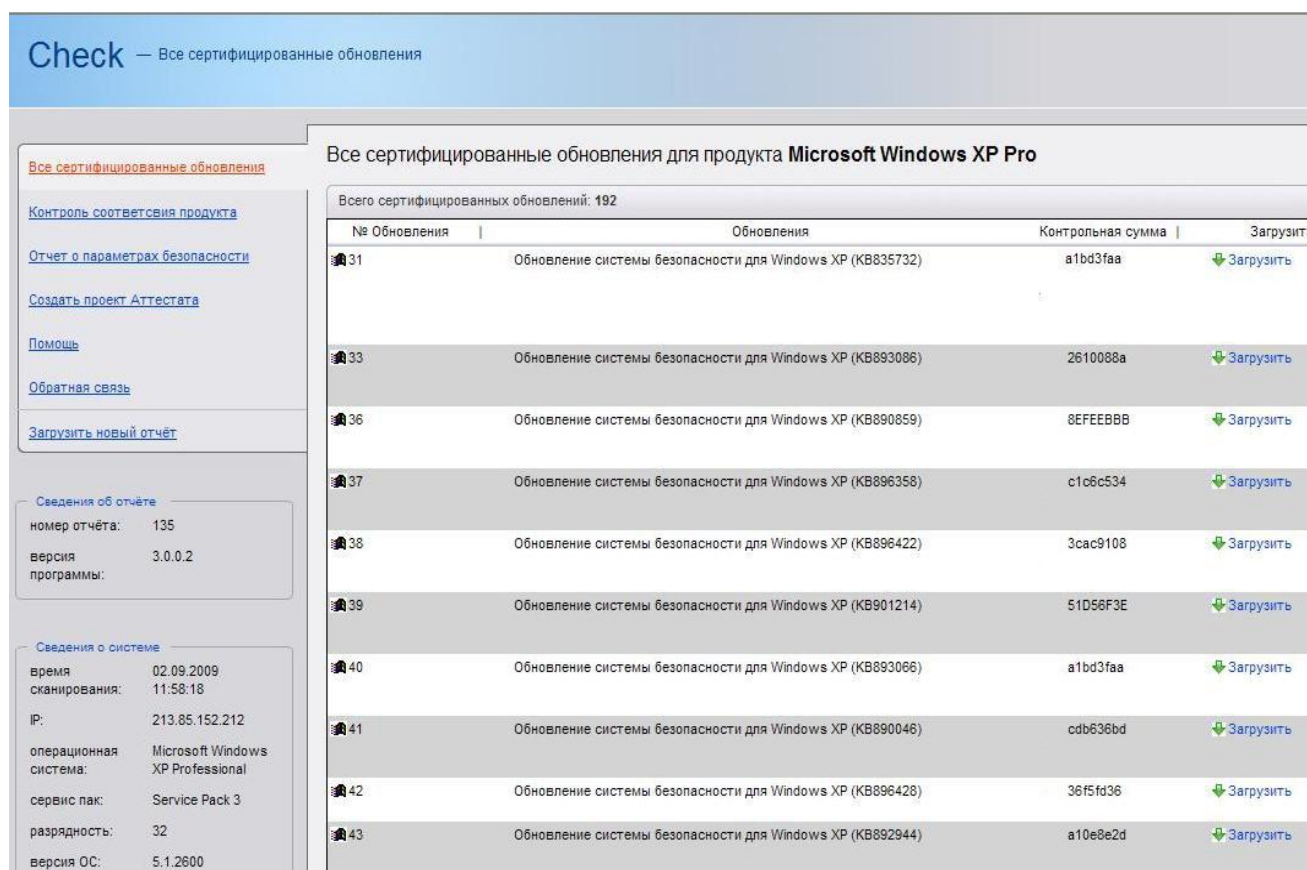


Рисунок 3.13 – Вид окна программы контроля сертифицированной версии Microsoft® Windows® XP Professional после выбора вкладки «Все сертифицированные обновления»

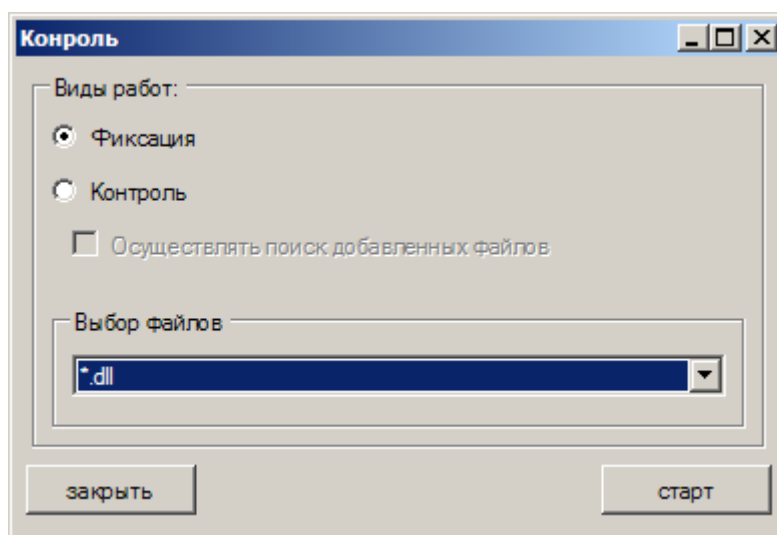



Рисунок 3.14 – Вид окна программы при проведении фиксации или контроля исходного состояния файлов ОС Microsoft® Windows® XP Professional

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 3.15.

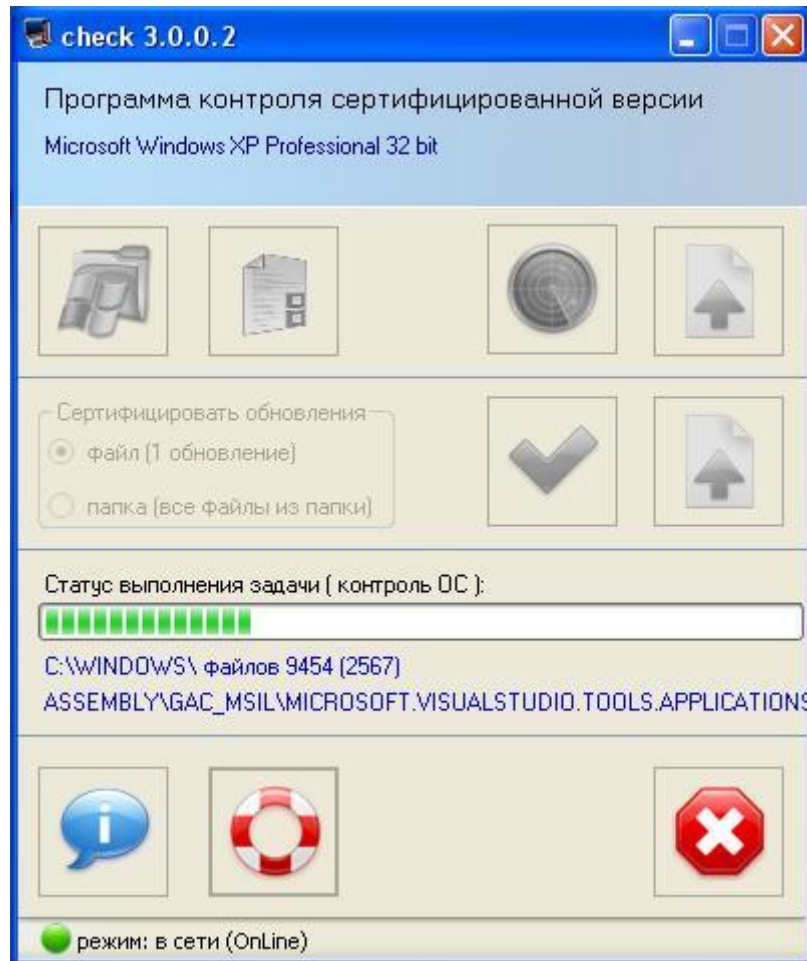


Рисунок 3.15 – Вид окна программы при проведении контроля исходного состояния файлов ОС Microsoft® Windows® XP Professional

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 3.16. В автоматически открывающемся окне будет представлен обобщенный результат контроля – количество проконтролированных файлов, количество измененных файлов, количество

**Руководство по безопасной настройке и контролю сертифицированной версии**

отсутствующих файлов, добавленных в системную папку (только при установленном флажке «Осуществлять поиск добавленных файлов»).

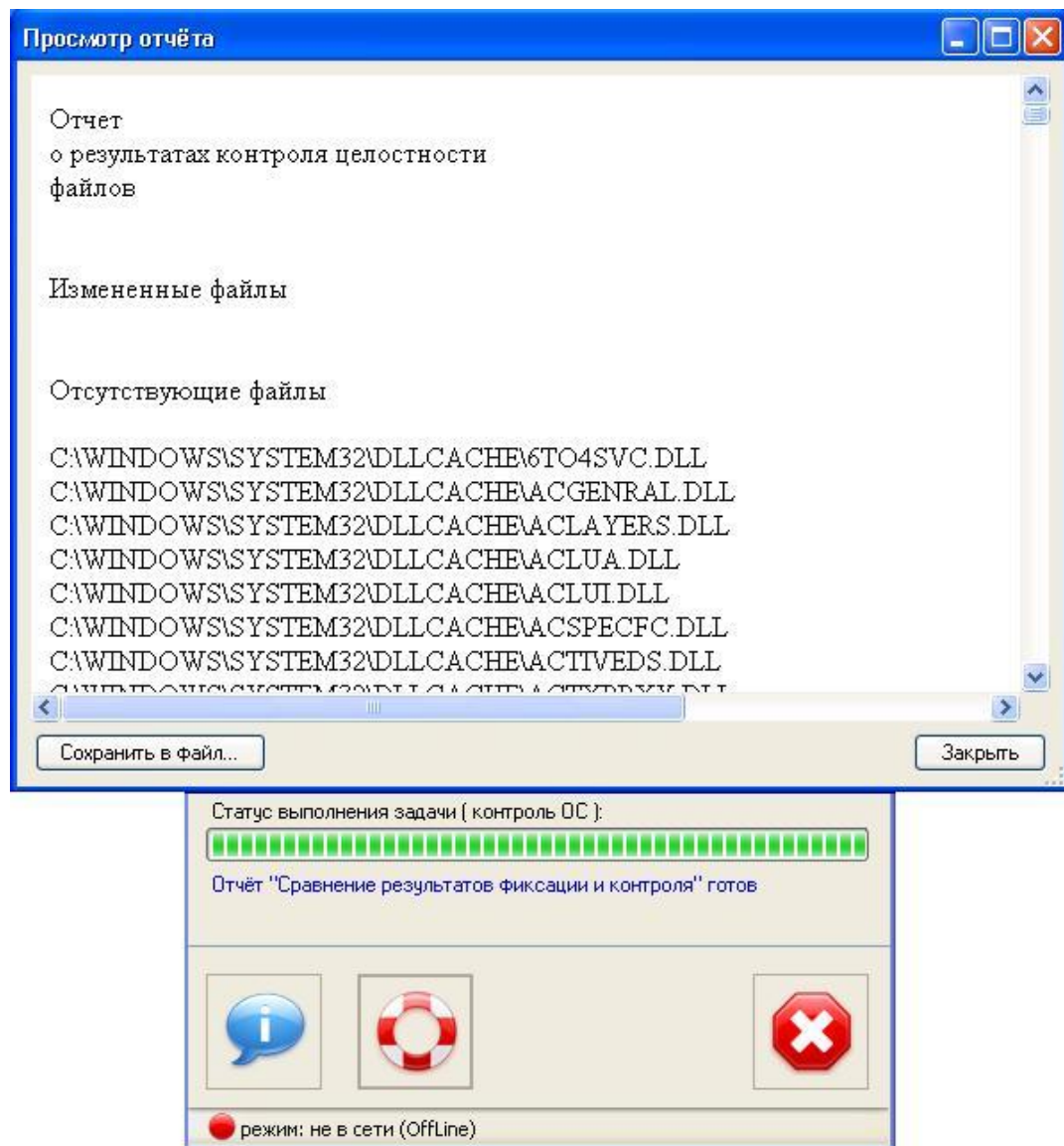


Рисунок 3.16 – Вид окна программы при проведении контроля исходного состояния файлов ОС Microsoft® Windows® XP Professional

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 Аттестаата соответствия необходимо нажать кнопку «Создать проект Аттестаата» в главном окне программы. После заполнения необходимых полей, в появившемся окне, вид которого представлен на рисунке 3.17, необходимо нажать кнопку «Далее». Если какое-либо поле останется незаполненным, то в проекте Аттестаата 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 Аттестаата и записи его в файл в формате HTML необходимо нажать кнопку «Далее».

Контроль

Проект аттестата

Для создания аттестата заполните нижеуказанные поля

Полное наименование автоматизированной системы  
Рабочее место контроля и учета персональных данных ЗАО "Контроль-плюс"

№ акта: 1      Дата выдачи акта: 28 июля 2009 г.      Срок действия (лет): 5      Класс защищённости системы: 1Д

Контроль за эффективностью мер защиты возлагается на (должность и подразделение)  
начальника службы безопасности ЗАО "Контроль-плюс"

Должность и наименование организации руководителя аттестационной комиссии  
Директор ЗАО "Контроль-плюс"


Класс защищённости системы  
И.И. Иванов

Заключение аттестационной комиссии, номера программы и методики испытаний

№: 1      Дата: 28 июля 2009 г.      № программы: 2      № методики испытаний: 3

пример      сброс      назад      далее

Рисунок 3.17 – Вид окна программы контроля сертифицированной версии Windows XP в режиме создания проекта Аттестаата соответствия после нажатия кнопки «пример»

Для создания проекта Аттестаата 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 аттестат соответствия».

При соответствии файлов сертифицированной ОС Microsoft® Windows® XP Professional, но несоответствии настроек параметров безопасности контролируемой системы рекомендуемым параметрам, вкладка «отчет о параметрах безопасности», будет иметь вид, представленный на рисунке 3.18.

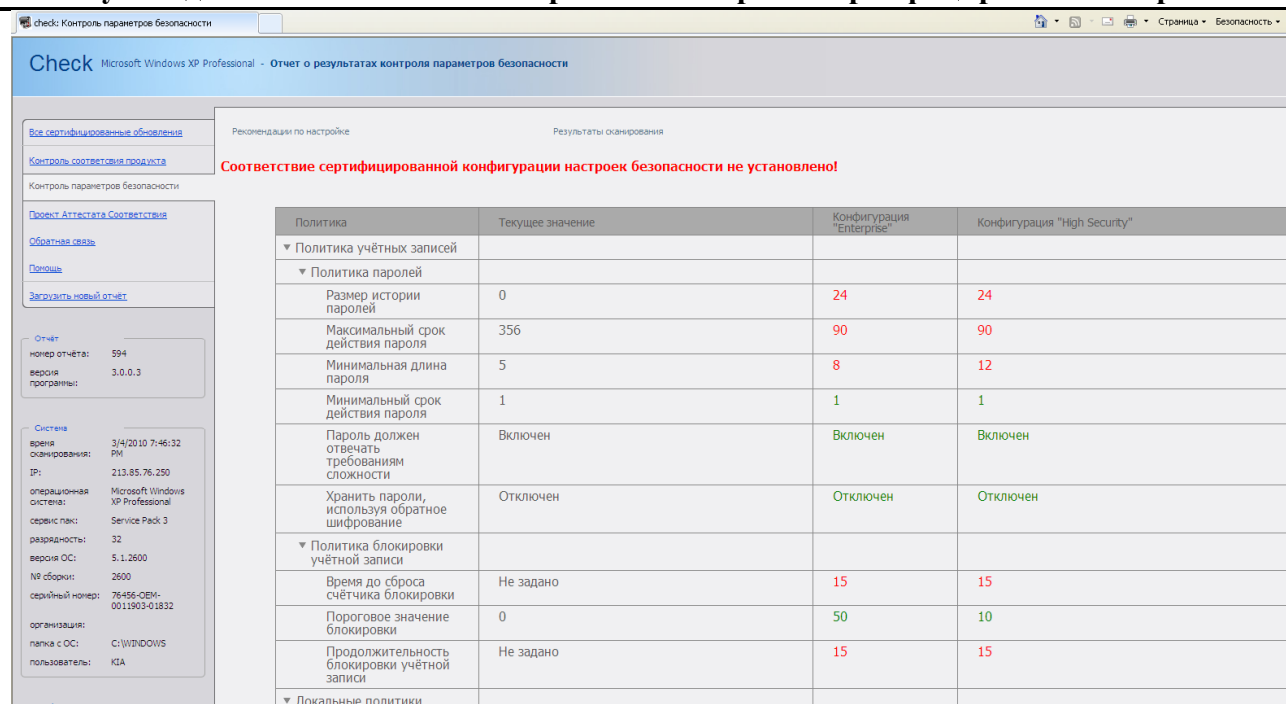


Рисунок 3.18 – Вид окна программы контроля сертифицированной версии ОС Microsoft® Windows® XP Professional при несоответствии настроек параметров безопасности рекомендуемым

### 3.3 Поиск и диагностика неисправностей программы «XP\_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 «XP\_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](mailto:support@altx-soft.ru) для диагностики неисправности.

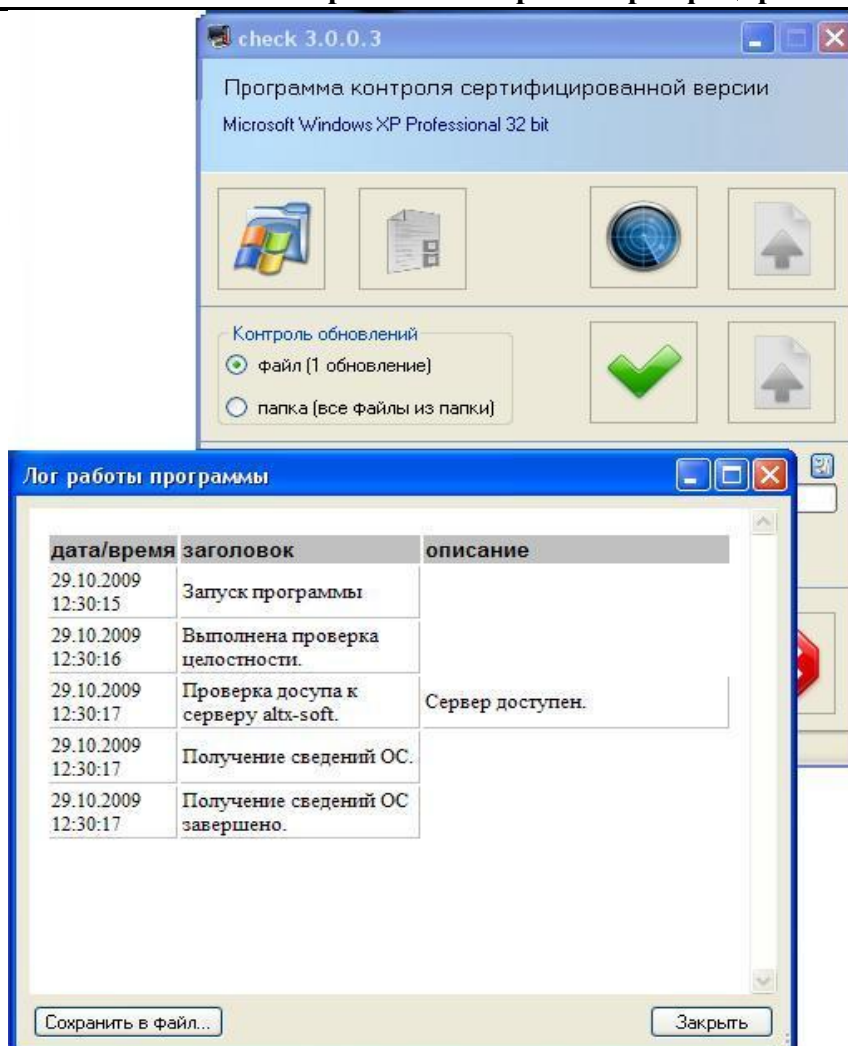


Рисунок 3.19 – Вид информационного окна программы, содержащей техническую информацию, при отсутствии доступа к серверу контроля.

## А.1 Групповая политика

Цель политик безопасности – определить процедуры выбора конфигурации и управления безопасностью в среде функционирования. Групповая политика помогает применить технические рекомендации в политике безопасности для всех клиентских 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 настольных компьютерных систем путем выборочного включения и выключения отдельных функций.

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 (OU), а затем назначать группам единые параметры конфигурации, что обеспечит непротиворечивость конфигураций разных членов групп. Использование групповой политики в сочетании со структурой организационных подразделений OU позволяет определять специфические настройки безопасности для тех или иных функций конкретного клиентского компьютера или сервера.

В случае использования групповой политики для создания настроек безопасности, любые изменения, осуществляемые по отношению к какой-либо из политик, будут относиться ко всем серверам и клиентским компьютерам, использующим эту политику.

Параметры групповой политики хранятся в следующих местах:

- контейнерах групповой политики Group Policy Container (GPC), расположенных в Active Directory;
- шаблонах групповой политики Group Policy Template (GPT), размещенных в файловой системе.

## **А.2 Рекомендованные параметры безопасности клиентских компьютеров под управлением операционной системы Microsoft® Windows® XP Professional**

Рекомендованные параметры безопасности, представленные в данной главе, учитывают особенности конфигураций «Enterprise» и «High Security». В данном разделе рассматриваются основные рекомендованные параметры безопасности, для настройки которых в домене Active Directory используется групповая политика. Применение рекомендованных параметров позволяет защитить информацию, обрабатываемую на клиентских персональных компьютерах (ПК) 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 OU, которое содержит контроллер 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 нарушителю возможность организации атак различных типов, направленных на подбор пароля.

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 групповой политики необходимо настроить параметры политики паролей в следующем разделе пространства имен объекта групповой политики: 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® XP Professional

Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
Максимальный срок действия пароля	90 дней	90 дней
Минимальная длина пароля	8 символов	12 символов
Минимальный срок действия пароля	1 день	1 день
Пароль должен отвечать требованиям сложности	Включен	Включен
Требовать неповторяемости паролей	24 хранимых пароля	24 хранимых пароля
Хранить пароли всех пользователей в домене, используя обратимое шифрование	Отключен	Отключен

Параметр безопасности «Максимальный срок действия пароля» ограничивает период времени, в течение которого нарушитель, подобравший пароль пользователя, сможет получать доступ к его компьютеру. Значение данного интервала может находиться в диапазоне от 0 до 999 дней.

Для двух типов конфигураций необходимо установить значение данного параметра равным «90 дней». Подобрать можно почти любой пароль, следовательно, чем чаще пароль изменяется, тем меньше у нарушителя 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 значения параметра «Максимальный срок действия пароля» равным «90 дней» позволит обеспечить регулярность смены пароля, повышая тем самым безопасность его использования.

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

Использование 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 нарушителем 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. 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 поддержки. Кроме того, использование слишком длинных паролей может привести к фактическому снижению безопасности, потому что пользователи из боязни забыть пароль вынуждены его записывать.

С другой стороны, увеличение длины пароля на один символ приводит к экспоненциальному повышению его надежности. Использование паролей длиной не менее 8 символов приводит к значительному усилению даже менее надежного механизма хеширования паролей LMHash, потому что в этом случае злоумышленнику необходимо взломать две части каждого пароля.

Исходя из этого, в конфигурации «Enterprise» значение параметра «Минимальная длина пароля» должно равняться «8 символов». Пароли такой длины позволяют обеспечить соответствующий уровень безопасности и сравнительно легко запоминаются пользователями. В конфигурации «High Security» должны использоваться пароли длиной не менее 12 символов.

Параметр безопасности «Минимальный срок действия пароля» устанавливает длительность периода времени использования пароля до того, как пользователь получает право его сменить. Значение параметра может находиться в диапазоне от 1 до 998 дней. Чтобы разрешить пользователю менять пароль немедленно, используется значение 0.

Только при значениях данного параметра, отличных от нуля, обеспечивается эффективность использования параметра «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 соответствует этой рекомендации, поэтому для двух типов конфигураций необходимо 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 базовым требованиям, которые предъявляются к их надежности. Увеличение длины пароля на один символ приводит

к экспоненциальному повышению сложности его подбора. Например, использование 7-значного пароля означает  $1 \times 10^7$  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  $2 \times 10^{11}$  комбинаций. При скорости 1 000 000 подстановок в секунду (показатель многих программ для определения паролей), все возможные комбинации будут проверены через 59 часов. Использование символов, вводимых с помощью клавиши ALT, и других специальных символов (например ! или @) значительно увеличивает промежуток времени, необходимый для подбора пароля. Совместное использование описанных символов значительно усложняет осуществление атак нарушителем. Поэтому для обеих конфигураций 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 двух типов конфигураций безопасности необходимо установить значение данного параметра равным «24 хранимых пароля». Установка максимального значения («24 хранимых пароля» является максимально возможным значением) предотвращает повторное (случайное или преднамеренное) использование 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 использование операционной системой обратимого шифрования при сохранении паролей. Этот параметр обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранение паролей, используя обратимое шифрование, 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, в обеих конфигурациях эту возможность необходимо отключить.

### ***Политика блокировки учетной записи***

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

С целью предотвращения возможности подбора пароля злоумышленником и снижения вероятности получения несанкционированного доступа к сети с помощью редактора групповой политики необходимо настроить параметры политики блокировки учетной записи в следующем разделе пространства имен объекта групповой политики: 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® XP Professional

Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
Блокировка учетной записи на	15 минут	15 минут
Пороговое значение блокировки	50 ошибок входа	10 ошибок входа
Сброс счетчика блокировки через	15 минут	15 минут

Параметр безопасности «Блокировка учетной записи на» служит для определения периода времени, по прошествии которого пользователь может повторить попытку входа в систему. В течение указанного периода времени учетная запись будет не доступна. В случае если значение параметра установлена равным нулю, учетная запись будет недоступна до тех пор, пока администратор не разблокирует ее.

Установка значения параметра «Блокировка учетной записи на» равное «15 минут» обеспечивает достаточную безопасность системы, не вызывая увеличения

**Руководство по безопасной настройке и контролю сертифицированной версии**

количества обращений в службу поддержки пользователей сети. Поэтому в обеих конфигурациях для данного параметра должно быть установлено значение «15 минут».

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. Уполномоченные пользователи могут заблокировать свои учетные записи, неправильно введя собственный пароль. Поэтому чтобы избежать блокировки учетных записей уполномоченных пользователей необходимо установить высокое пороговое значение блокировки. Для конфигурации «Enterprise» рекомендуется установить значение блокировки равным «50 ошибок входа в систему», для «High Security» - «10 ошибок входа в систему».

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 двух конфигураций рекомендуется установить значение параметра «Сброс счетчика блокировки через» равное «15 минутам».

В случае, когда клиентский компьютер является автономным компьютером в конфигурациях «Enterprise» или «High Security» и функционирует в домене на базе Active Directory или в домене Windows NT 4.0, 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 непосредственно на каждом компьютере под управлением операционной системы Microsoft® Windows® XP Professional

или централизованно для всего множества компьютеров, функционирующих в заданной конфигурации. Для этого используется соответственно локальная политика безопасности или 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***

С помощью политики аудита определяются события безопасности, которые включаются в соответствующий отчет. В результате этого создается журнал регистрации определенных действий системы и пользователей (далее – журнал регистрации событий). 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 с ее помощью. 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 настройками аудита назначено отслеживание большого количества разрешенных действий, журнал регистрации событий безопасности будет переполнен бесполезной информацией. Приведенные далее рекомендации помогут взвешенно подойти к определению отслеживаемых действий и метода сбора данных.

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® XP Professional

Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
Аудит событий входа в систему	Успех	Успех, отказ

Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
Аудит управления учетными записями	Успех	Успех, отказ
Аудит доступа к службе каталогов	Нет аудита	Нет аудита
Аудит входа в систему	Успех	Успех, отказ
Аудит изменения политики	Успех	Успех
Аудит использования привилегий	Отказ	Отказ
Аудит системных событий	Успех	Успех

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 системы Microsoft® Windows® XP Professional . Для конфигурации «Enterprise», параметр «Аудит событий входа в систему» должен иметь значение «Успех», а для «High Security» - «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 «High Security» - «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. Данный параметр не применяется к компьютерам под управлением операционной системы Microsoft® Windows® XP Professional .

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® XP Professional . Для конфигурации «Enterprise», параметр «Аудит входа в систему» должен иметь значение «Успех», а для «High Security» - «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.

Исходя из этого, для двух типов конфигураций параметр «Аудит изменения политики» должен иметь значение «Успех». Добавление значения «Отказ» не приведет к появлению в журнале регистрации событий сведений, имеющих практическую ценность.

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 обеих конфигураций безопасности. 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

**Руководство по безопасной настройке и контролю сертифицированной версии**

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 «High Security», 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® XP Professional 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® XP Professional

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
1.	Доступ к компьютеру из сети	Администраторы, Пользователи	Администраторы, Пользователи
2.	Работа в режиме операционной системы	Никто (No One)	Никто (No One)
3.	Настройка квот памяти для процесса	Не определено	Администраторы, Локальная служба, Сетевая служба



## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
4.	Локальный вход в систему	Администраторы, Пользователи	Администраторы, Пользователи
5.	Удаленный вход в систему (разрешать вход в систему через службу терминалов)	Не определено	Никто (No One)
6.	Архивирование файлов и каталогов	Не определено	Администраторы
7.	Изменение системного времени	Администраторы	Администраторы
8.	Создание страничного файла (pagefile)	Администраторы	Администраторы
9.	Создание постоянных объектов совместного использования	Не определено	Никто
10.	Создание маркерного объекта	Не определено	Никто
11.	Отладка программ	Администраторы	Никто
12.	Отказ в доступе к компьютеру из сети	Гость Support_388945a0	Группа:Гости Support_388945a0
13.	Отклонить локальный вход	Не определено	Гость Support_388945a0
14.	Запретить вход в систему через службу терминалов	Не определено	Все
15.	Разрешение доверия к учетным записям при делегировании	Не определено	Никто
16.	Принудительное удаленное завершение	Администраторы	Администраторы
17.	Создание журналов безопасности	Локальная служба, Сетевая служба	Локальная служба, Сетевая служба
18.	Увеличение приоритета диспетчеризации	Администраторы	Администраторы
19.	Загрузка и выгрузка драйверов устройств	Администраторы	Администраторы
20.	Вход в качестве пакетного задания	Не определено	Никто

## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
21.	Вход в качестве службы	Не определено	Локальная служба, Сетевая служба
22.	Управление аудитом и журналом безопасности	Администраторы	Администраторы
23.	Изменение параметров среды оборудования	Администраторы	Администраторы
24.	Запуск операций по обслуживанию тома	Администраторы	Администраторы
25.	Профилирование одного процесса	Не определено	Администраторы
26.	Профилирование загрузки системы	Администраторы	Администраторы
27.	Замена маркера уровня процесса	Локальная служба, Сетевая служба	Локальная служба, Сетевая служба
28.	Восстановление файлов и каталогов	Не определено	Администраторы
29.	Завершение работы системы	Администраторы, Пользователи	Администраторы, Пользователи
30.	Овладение файлами или иными объектами	Администраторы	Администраторы
31.	Добавление рабочих станций к домену	Администраторы	Администраторы
32.	Отказ во входе в качестве пакетного задания	Не задано	Группа: Гости Support_388945a0
33.	Олицетворение клиента после проверки подлинности	Не задано	Группа: все участники безопасности, вошедшие в систему в качестве службы. Принадлежность контролируется операционной системой(СЛУЖБА), Локальная служба, Сетевая служба, Группа: администраторы

## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
34.	Закрепление страниц в памяти	Не задано	Не задано
35.	Извлечение компьютера из стыковочного узла	Администраторы, Пользователи	Администраторы, Пользователи

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 «Enterprise» данное право следует предоставить группам «Администраторы» и «Пользователи», так же и в конфигурации «High Security» - «Администраторы» и «Пользователи».

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 обеих конфигурациях безопасности 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 «High Security» право «Увеличение квоты, назначенной на процесс» 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.

В общем случае данную привилегию следует предоставлять только группам «Администраторы» и «Пользователи».

Параметр «Удаленный вход в систему» (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 «High Security» использование данного права запретить для всех (значение «No One» – Никто).

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 «High Security», данное право, определяющее границы доступа к файлам и папкам на клиентских компьютерах, необходимо предоставить только локальной группе «Администраторы».

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 обеих конфигурациях данным правом должны обладать только члены группы «Администраторы».

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 обеих конфигурациях 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 ОС Microsoft® Windows® XP Professional . Поскольку компоненты, работающие в режиме ядра, уже обладают этой привилегией, им не нужно специально назначать ее.

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

Параметр «Отладка программ» предоставляет пользователю 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», а в конфигурации «High Security» – «Никто».

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 заблокирован. Для обеспечения контролируемого доступа к совместно используемым ресурсам должны быть использованы файловые сервера.

В связи с этим, в конфигурации «High Security» доступа к рабочим станциям под управлением ОС Microsoft® Windows® XP Professional из сети наряду с анонимными пользователями, должны быть лишены пользователи, успешно прошедшие процедуры идентификации и аутентификации (значение «Support\_388945a0 и группа:Гости»).

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 «High Security» интерактивный локальный вход в систему должен быть запрещен с использованием учетных записей «Support\_388945a0» и «Гость», а также учетной записи, используемой для запуска служб операционной системы.

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 «Запрещен удаленный вход в систему» в конфигурации «High Security» должно быть предоставлено группе «Все», а в конфигурации «Enterprise» значение для данного параметра может быть не определено.

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 обеих конфигурации безопасности использование данной привилегии должно быть запрещено для всех пользователей (значение «No One» – Никто).

Право «Удаленное завершение работы системы» дает возможность пользователям дистанционно по сети отключать компьютеры под управлением операционной системы Microsoft® Windows® XP Professional . 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 конфигурациях «Enterprise» и «High Security» должно быть предоставлено только группе «Администраторы».

Право «Создание журналов безопасности» определяет, какие пользователи или процессы могут осуществлять запись данных аудита в журнал безопасности операционной

**Руководство по безопасной настройке и контролю сертифицированной версии**

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 обеих конфигурациях 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 конфигурациях «High Security» и «Enterprise» 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 конфигурациях «High Security» и «Enterprise» право «Загрузка и выгрузка драйверов устройств» должно быть предоставлено только участникам группы безопасности «Администраторы».

Наличие права «Вход в качестве пакетного задания» 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 конфигурации «High Security» использование данной привилегии должно быть запрещено для всех пользователей (значение «No One» – Никто).



Право «Вход в качестве службы» определяет, какие учетные записи служб могут зарегистрировать процесс в качестве службы. Использование данного права должно быть ограничено на любом компьютере под управление ОС Microsoft® Windows® XP Professional в конфигурации «High Security» но поскольку для функционирования многих приложений оно необходимо, то перед его присвоением требуется провести тщательный анализ возможных последствий его использования в заданной среде функционирования.

Таким образом, для реализации повышенных требований к безопасности, в конфигурации «High Security» использование данного права должно быть ограничено для всех пользователей, кроме «Локальной службы» и «Сетевой службы».

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 конфигурациях «High Security» и «Enterprise» 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 конфигурациях «High Security» и «Enterprise» 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 конфигурациях «High Security» и «Enterprise» 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 «High Security» должно быть предоставлено группе «Администраторы», а в конфигурации «Enterprise» значение для данного параметра может быть не определено.

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 «High Security» должно быть предоставлено группе «Администраторы», а в конфигурации «Enterprise» значение для данного параметра может быть не определено.

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 обеих конфигурациях безопасности 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® XP Professional . 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 «High Security» должно быть предоставлено группе «Администраторы», а в конфигурации «Enterprise» значение для данного параметра может быть не определено.

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, в конфигурациях «High Security» и «Enterprise» данное право должно предоставляться только группам «Администраторы» и «Пользователи».

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, обладающему им, действовать в обход прав доступа, установленных на объекте доступа и становиться его владельцем.

В конфигурациях «High Security» и «Enterprise» данное право должно быть предоставлено группе «Администраторы».

Пользователи, обладающие правом «Добавление рабочих станций к домену» могут включать новые компьютеры в состав домена Active Directory. Пользователи, входящие в группу «Прошедшие проверку», могут добавлять до 10 учетных записей компьютеров в домен Active Directory. Кроме того, включать компьютеры в состав домена могут пользователи, обладающие правом создания объекта типа «Компьютер» для контейнера «Computers» в каталоге Active Directory. Такие пользователи могут добавить в домен неограниченное число компьютеров (независимо от того, присвоено ли им право «Добавление рабочих станций в домен»).

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».

Данные параметры позволяют включать и отключать параметры безопасности компьютера и по существу позволяют пользователям операционной системы Microsoft® Windows® XP Professional 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® XP Professional, 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® XP Professional

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
1.	Учетные записи: ограничить использование пустых паролей только для консольного входа	Включен	Включен
2.	Устройства: разрешать отстыковку без входа в систему	Не определено	Отключен
3.	Устройства: разрешено форматировать и извлекать съемные носители	Администраторы, Интерактивные пользователи	Администраторы
4.	Устройства: запретить пользователям установку драйверов принтера	Включен	Включен
5.	Устройства: разрешить доступ к дисковым компакт-дискам только локальным пользователям	Не определено	Отключен

## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
6.	Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям	Не определено	Отключен
7.	Член домена: отключить изменение пароля учетных записей компьютера	Отключен	Отключен
8.	Член домена: цифровая подпись безопасного канала, когда это возможно	Включен	Включен
9.	Член домена: шифрование данных безопасного канала, когда это возможно	Включен	Включен
10.	Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала	Включен	Включен
11.	Член домена: максимальный срок действия пароля учетных записей компьютера	30 дней	30 дней
12.	Член домена: требует стойкого ключа сеанса (Windows 2000 или выше)	Включен	Включен
13.	Интерактивный вход в систему: не отображать последнего имени пользователя	Включен	Включен
14.	Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL	Отключен	Отключен
15.	Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)	2	0
16.	Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее	14 дней	14 дней
17.	Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера	Включен	Включен
18.	Интерактивный вход в систему: поведе-	Блокировка рабочей	Блокировка рабо-

## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
	ние при извлечении смарт-карты	станции	чей станции
19.	Клиент сети Microsoft: использовать цифровую подпись (всегда)	Включен	Включен
20.	Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	Включен	Включен
21.	Клиент сети Microsoft: посылать незашифрованный пароль сторонним SMB-серверам	Отключен	Отключен
22.	Сервер сети Microsoft: длительность простоя перед отключением сеанса	15 минут	15 минут
23.	Сервер сети Microsoft: использовать цифровую подпись (всегда)	Включен	Включен
24.	Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)	Включен	Включен
25.	Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа	Включен	Включен
26.	Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями	Включен	Включен
27.	Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями	Включен	Включен
28.	Сетевой доступ: не разрешать сохранение учетных данных или цифровых паспортов .NET для сетевой проверки подлинности пользователя	Включен	Включен
29.	Сетевой доступ: разрешать применение разрешений для всех к анонимным пользователям	Отключен	Отключен
30.	Сетевой доступ: разрешать анонимный доступ к общим ресурсам	Не определено	comcfg, dfs\$

## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
31.	Сетевой доступ: разрешать анонимный доступ к именованным каналам	Не определено	Источник доступа:COMNAP COMNODE SQL\QUERY SPOOLSS EPMAPPER LOCATOR TrkWks TrkSvr
32.	Сетевой доступ: удаленно доступные пути и вложенные пути реестра	Не определено	список:  System\CurrentControlSet\ Control\ProductOptions System\CurrentControlSet\ Control\Print\Printers System\CurrentControlSet\ Control\Server ApplicationsSystem\Curre ntControlSet\Services\Eve ntlog  Software\Microsoft\OLAP ServerSoftware\Microsoft\ WindowsNT\CurrentVersi on\System\CurrentControl Set\Control\ContentIndex System\CurrentControlSet\ Control\Terminal Server System\CurrentControlSet\ Control\Terminal Server\UserConfig System\CurrentControlSet\ Control\Terminal Server\DefaultUserConfig uration
33.	Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей	Обычная - локаль- ные пользователи удостоверяются как они сами	Обычная - локаль- ные пользователи удостоверяются как они сами
34.	Сетевая безопасность: не хранить хеш-значений LAN Manager при следующей смене пароля	Включен	Включен
35.	Сетевая безопасность: уровень проверки	Запрет контроллеру	Необходимость

## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
	подлинности LAN Manager	домена использовать аутентификацию LM (отправлять только NTLMv2- ответ)	применять при аутентификации только протокол NTLMv2 (отказывать LM и NTLM)
36.	Сетевая безопасность: требования подписывания для LDAP-клиента	Согласование подписывания	Согласование подписывания
37.	Сетевая безопасность: минимальная сетевая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)	Требовать 128- разрядное шифрование, Требовать сеансо- вую безопасность NTLMv2.	Требовать 128- разрядное шифрование, Требовать сеансо- вую безопасность NTLMv2.
38.	Сетевая безопасность: минимальная сетевая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)	Требовать 128- разрядное шифрование, Требовать сеансо- вую безопасность NTLMv2.	Требовать 128- разрядное шифрование, Требовать сеансо- вую безопасность NTLMv2.
39.	Консоль восстановления: разрешить автоматический вход администратора	Отключен	Отключен
40.	Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам	Не определено	Отключен
41.	Завершение работы: разрешить завершение работы системы без выполнения входа в систему	Не определено	Отключен
42.	Завершение работы: очистка страничного файла виртуальной памяти	Отключен	Отключен



## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
43.	Системные объекты: владелец по умолчанию для объектов, созданных членами группы администраторов	Создатель объекта	Создатель объекта
44.	Системные объекты: учитывать регистр для подсистем, отличных от Windows	Не определено	Включен
45.	Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок)	Включен	Включен
46.	Аудит: аудит доступа глобальных системных объектов	Отключен	Отключен
47.	Аудит: аудит прав на архивацию и восстановление	Не определено	Отключен
48.	Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности	Не определено	Отключен
49.	Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания	Не определено	Отключен
50.	Автоматический вход в систему	Не определено	Отключен
51.	Запрет IP маршрутизации от источника	Не определено	Отключен
52.	Механизм определения 'мертвых' шлюзов	Не определено	Отключен
53.	Скрыть компьютер из списка просмотра (Browse List)	Не определено	Включен
54.	Изменение таблицы маршрутизации в ответ на ICMP-редирект пакеты	Не определено	Отключен

## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
55.	Интервал отправки пакетов проверки активности соединения	Не определено	300000 миллисекунд
56.	Запретить привилегированный трафик для протоколов Kerberos и RSVP	Kerberos и RSVP трафик не освобождаются от IPSec-фильтрации, но многоадресные передачи, трансляции и ISAKMP трафик освобождаются	Kerberos и RSVP трафик не освобождаются от IPSec-фильтрации, но многоадресные передачи, трансляции и ISAKMP трафик освобождаются
57.	Не производить показ NetBIOS имени компьютера	Не определено	Включен
58.	Запрет на создание коротких NetBIOS имен	Не определено	Включен
59.	Использование IRDP-протокола	Не определено	Включен
60.	Защита от SYN-атак (защищает от DoS:Тайм-аут раньше, если SYN атака обнаружена)	Не определено	Включен
61.	Установка времени тайм-аута (количество перепередач пакетов с флагами SYN и ACK)	Не определено	повтор SYN ACK через 3,6 секунд, очистка очереди через 12 секунд после отправки последнего ответа, T = 21 с.
62.	Количество неудачных попыток передачи данных, перед разрывом соединения	Не определено	3 раза
63.	Предельный размер (в процентном соотношении) журнала событий, по достижении которого система будет формировать предупреждение	Не определено	90 процентов
64.	Возможность передачи пакетов при помощи флага маршрутизации от источника	Не определено	Источник направляющий маршрутизацию полностью отключен

№ п/п	Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
65.	Количество попыток повторной передачи пакетов с флагами SYN и ACK	Не определено	3 раза

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 конфигурации «High Security» 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 конфигурации «Enterprise» должен иметь значение «Администраторы и интерактивные пользователи», а в конфигурации «High Security» - «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 интерактивный вход в систему. В тоже время, если данный параметр активирован, но никто не выполнил локальный вход в систему, дисковод компакт-дисков может быть доступен удаленным пользователям.

По этой причине, в конфигурации безопасности «Enterprise» данный параметр может иметь значение «Не определен», а в конфигурации «High Security» 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 интерактивный вход в систему. В тоже время, если данный параметр активирован, но никто не выполнил локальный 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 «High Security» принимает значение «Отключен».

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 «High Security» 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 «High Security» максимальный срок действия пароля учетных записей компьютера должен быть равен 30 дням.

Параметр безопасности «Интерактивный вход в систему: не отображать последнего 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 «Включен».

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 контроллеру домена. При значении параметра, равном 2, пользователи, которые не могут связаться с контроллером домена, имеют возможность войти в систему с помощью сохраненных учетных данных. При значении параметра, равном 1, на клиентском компьютере хранится только один набор учетных данных. Если еще кому-то потребуется использовать этот компьютер, его надо будет подключить к сети, чтобы контроллер домена проверил подлинность учетных данных дополнительного пользователя.

Исходя из этого, в конфигурации «Enterprise» для параметра должно быть установлено значение «2», а для конфигурации «High Security» 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 получают 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 конфигурации «Enterprise» необходимо отключить данный параметр, а в конфигурации «High Security» включить.

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 включения режима подписи SMB на самом клиенте.

Активирование данного параметра безопасности должно быть осуществлено в конфигурациях «Enterprise» и «High Security», поскольку в этом случае предъявляются повышенные требования к безопасности.

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: длительность простоя перед отключением 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® XP Professional 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: длительность простоя перед отключением сеанса» 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 «Доступ к сети: Разрешить трансляцию анонимного SID в имя» определяет, может ли анонимный пользователь запросить атрибуты идентификатора безопасности SID (Security Identifier) другого пользователя или использовать этот идентификатор для получения соответствующего имени. Отключение этого параметра не позволит получать имена пользователей по соответствующим идентификаторам безопасности SID.

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: разрешать применение разрешений для всех к анонимным пользователям» определяет, какие дополнительные разрешения предоставляются при анонимном подключении к компьютеру. Microsoft® Windows® XP Professional 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 поддерживаются 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 «High Security» данному параметру должны быть присвоены значения «comcfg» и «dfs\$». 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 «Сетевая безопасность: принудительный вывод из сеанса 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® XP Professional . 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® XP Professional , 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», а для конфигурации «High Security» - значению «Необходимость применять при аутентификации только протокол NTLMv2».

Параметр безопасности «Сетевая безопасность: требования подписывания 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 «High Security» 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® XP Professional 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

**Руководство по безопасной настройке и контролю сертифицированной версии**

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 «Не определено». В свою очередь, в конфигурации «High Security» 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 конфигурации «Enterprise» данный параметр может принимать значение «Не определено». В свою очередь, в конфигурации «High Security» 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 «High Security» данный параметр может быть отключен.

Параметр безопасности «Системные объекты: владелец по умолчанию для объектов, созданных членами группы администраторов» определяет, какая из групп будет по умолчанию назначена владельцем новых системных объектов – «Администраторы» или «Создатель объекта». Использование для этого параметра значения «Администраторы» сделает невозможным хранение отдельных учетных данных для создания новых системных объектов. С целью отражения учетной записи, создавшей объект, в отличие от более общей группы «Администраторы», следует установить для параметра в обеих конфигурациях значение «Создатель объекта».

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 различие 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 конфигурации «High Security» 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 (Discretionary 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» групповой политики определяются атрибуты, относящиеся к журналам «Приложение», «Безопасность» и «Система»: 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® XP Professional

Название параметра	Конфигурация «Enterprise»	Конфигурация «High Security»
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

<b>Название параметра</b>	<b>Конфигурация «Enterprise»</b>	<b>Конфигурация «High Security»</b>
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 функционированием 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 конфигурации «High Security» размер журнала безопасности должен быть увеличен. Поэтому в конфигурациях «Enterprise» и «High Security» для данного параметра рекомендуется значение 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, исходя из этого данные параметры в обеих конфигурациях 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. Данный 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 в обеих рассматриваемых конфигурациях 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 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 в операционной системе Microsoft® Windows® XP Professional . При вводе ограничений доступа для групп следует исходить из существующих потребностей. В данном руководстве для конфигурации «High Security» к группам с ограниченным доступом отнесена группа «Опытные пользователи». Несмотря на то, что члены группы «Опытные пользователи» имеют меньше возможностей доступа к системе, чем члены группы «Администраторы», тем не менее, спектр предоставленных им прав достаточно широк. Если в структуре организации задействована группа «Опытные пользователи», необходимо тщательно контролировать состав этой группы.

Членство в группах с ограниченным доступом следует настраивать в операционной системе Microsoft® Windows® XP Professional 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. Ограничения на доступ для групп вводятся только с помощью шаблонов безопасности.

В конфигурации «High Security» с целью полного ограничения доступа к группе «Опытные пользователи» должны быть удалены все пользователи и группы, входящих в нее. Рекомендуется вводить ограничения для всех встроенных групп, которые не планируется использовать на предприятии. В конфигурации «High Security» ввод ограничений для группы «Опытные пользователи» обусловлен тем, что права, предоставленные этой группе, почти

эквивалентны правам администраторов на компьютерах под управлением операционной системы Microsoft® Windows® XP Professional .

### **Системные службы**

При установке операционной системы Microsoft® Windows® XP Professional 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 любые ненужные службы или исполняемые файлы следует отключить или удалить.

Параметры системных служб следует настраивать в операционной системе Microsoft® Windows® XP Professional в редакторе групповой политики в следующем разделе пространства имен объекта групповой политики: Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Системные службы.

Параметры настройки системных служб операционной системы Microsoft® Windows® XP Professional , используемой в двух конфигурациях, представлены в таблице А.2.7.

Таблица А.2.7 – Параметры настройки системных служб для компьютеров под управлением операционной системы Microsoft® Windows® XP Professional

№ п/п	Системная служба	Имя службы	Режим запуска службы	
			Конфигурация «Enterprise»	Конфигурация «High Security»
1.	Оповещатель	Alerter	Отключен	Отключен
2.	Сервер папки обмена	ClipSrv	Отключен	Отключен
3.	Обозреватель компьютеров	Browser	Не определено	Отключен
4.	Служба факсов	Fax	Вручную	Отключен
5.	Служба FTP-публикации	MSFtpsvr	Отключен	Отключен
6.	Служба IIS Admin	IISADMIN	Отключен	Отключен
7.	Служба индексирования	cisvc	Отключен	Отключен
8.	Служба сообщений	Messenger	Отключен	Отключен
9.	NetMeeting Remote Desktop Sharing	mnmsrvc	Отключен	Отключен
10.	Служба сетевого DDE	NetDDE	Вручную	Отключен

## Руководство по безопасной настройке и контролю сертифицированной версии

№ п/п	Системная служба	Имя службы	Режим запуска службы	
			Конфигурация «Enterprise»	Конфигурация «High Security»
11.	Диспетчер сетевого DDE	NetDDEdsdm	Вручную	Отключен
12.	Диспетчер сеанса справки для удаленного рабочего стола	RDSessMgr	Не определено	Отключен
13.	Удаленный реестр	RemoteRegistry	Автоматически	Отключен
14.	Маршрутизация и удален- ный доступ	RemoteAccess	Отключен	Отключен
15.	Служба обнаружения SSDP	SSDPsrv	Отключен	Отключен
16.	Планировщик заданий	Schedule	Не определено	Отключен
17.	Служба Telnet	TlntSvr	Отключен	Отключен
18.	Службы терминалов	TermService	Не определено	Отключен
19.	Узел универсальных PnP- устройств	uPnPhost	Не определено	Отключен
20.	Служба веб-публикаций	W3SVC	Отключен	Отключен

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» в обеих конфигурациях должен быть установлен режим запуска «Отключен», который препятствует запуску данной службы и соответственно передаче данных по сети.

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 конфигураций «Enterprise» и «High Security» режим запуска для данной службы должен соответствовать значению «Отключен».

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 клиентскими 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 более высокого уровня безопасности служба «Обозреватель компьютеров» в конфигурации «High Security» должна быть отключена. В конфигурации «Enterprise» режим запуска данной службы определяется самостоятельно администратором безопасности.

«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 конфигурации «Enterprise» Службы факсов должна использовать режим запуска «Вручную». Однако чтобы обеспечить более высокую степень безопасности, в конфигурации «High Security» запуск данной службы должна 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® XP Professional, если в ней нет непосредственной необходимости. По этой причине в обеих конфигурациях, рассматриваемых в данном разделе руководства, Службу FTP-публикаций 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 клиентских компьютеров под управлением операционной системы Microsoft® Windows® XP Professional эти возможности не требуются. По этим причинам в обеих конфигурациях Служба IIS Admin должна быть отключена.

«Служба индексирования» индексирует содержимое и свойства файлов на локальном и удаленных компьютерах, обеспечивает быстрый доступ к файлам с помощью гибкого языка запросов. Служба индексирования также обеспечивает быстрый поиск документов на локальном и удаленных компьютерах. Чтобы обеспечить более высокий уровень безопасности для конфигураций «Enterprise» и «High Security» режим запуска для данной службы должен соответствовать значению «Отключен».

«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 клиентских компьютеров под управлением операционной системы Microsoft® Windows® XP Professional . По этим причинам в обеих конфигурациях Службу сообщений необходимо отключить.

Служба «NetMeeting Remote Desktop Sharing» разрешает авторизованным пользователям с помощью программы Microsoft NetMeeting® получать удаленный доступ к клиентскому 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 в конфигурациях «High Security» и «Enterprise» должен соответствовать значению «Отключен».

«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. По этой причине, чтобы обеспечить повышенный уровень безопасности, режим запуска данной службы в конфигурации «High Security» должен соответствовать значению «Отключен». Однако в конфигурации «Enterprise» для этой службы рекомендуется оставить значение по умолчанию – «Вручную».

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, чтобы обеспечить повышенный уровень безопасности режим запуска для данной службы в конфигурации «High Security» должен соответствовать значению «Отключен». Однако в конфигурации «Enterprise» для этой службы рекомендуется значение по умолчанию – «Вручную».

«Диспетчер сеанса справки для удаленного рабочего стола» управляет возможностями «Удаленного помощника» в Центре справки и поддержки операционной системы. После остановки данной службы «Удаленный помощник» будет недоступен. Чтобы обеспечить высокий уровень безопасности для конфигураций «Enterprise» и «High Security» данная служба должна быть отключена.

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. Чтобы блокировать доступ к реестру при функционировании компьютера в конфигурации «High Security» данную службу необходимо отключить. При отключении данной службы администратор должен вручную управлять получением обновлений на каждом компьютере или обеспечить пользователям возможность самостоятельной установки обновлений.

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 высокого уровня безопасности в конфигурациях «Enterprise» и «High Security» данная служба должна быть отключена.

«Служба обнаружения SSDP» обеспечивает возможность обнаружения и идентификации UPnP-устройств в вычислительной сети. Для этой цели данная служба использует протокол SSDP (Simple Service Discovery Protocol). Запрет функционирования Службы обнаружения SSDP позволит предотвратить поиск системой UPnP-устройств в вычислительной сети и прекратить взаимодействие и поддержку службой «Узел универсальных PnP-устройств» указанных устройств. В конфигурациях «Enterprise» и «High Security» данная служба должна быть отключена.

«Планировщик заданий» позволяет настраивать расписание автоматического выполнения задач на заданном клиентском 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, в конфигурации «High Security» данная служба должна быть отключена.

«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 клиентских компьютеров под управлением операционной системы Microsoft® Windows® XP Professional эта служба не является обязательной. По этой причине в обеих конфигурациях служба Telnet должна быть отключена.

«Службы терминалов» предоставляют возможность нескольким пользователям интерактивно подключаться к компьютеру и отображают рабочий стол и приложения на удаленных компьютерах как при интерактивной регистрации на компьютере. Для обеспечения высокого уровня безопасности в конфигурации «High Security» данная служба должна быть отключена.

Служба «Узла универсальных PnP-устройств» обеспечивает поддержку, регистрацию и управление универсальными PnP-устройствами, а также реакцию на события, связанными с обслуживаемыми устройствами. Универсальные PnP-устройства обладают способностью автоматической настройки сетевой адресации, анонсирования собственного присутствия в сети и обмена описаниями устройств. Таким образом, клиентский компьютер под управлением Microsoft® Windows XP Professional может выступать в качестве точки обнаружения и управления всеми UPnP-устройствами в сети.

Для обеспечения высокого уровня безопасности в конфигурации «High Security» данная служба должна быть отключена. В конфигурации «Enterprise» режим запуска данной службы определяется самостоятельно администратором безопасности.

«Служба веб-публикации» обеспечивает подключение и администрирование веб-узла с помощью оснастки IIS. Однако для большинства клиентских компьютеров под управлением операционной системы Microsoft® Windows® XP Professional эта служба не является обязательной. По этой причине в обеих конфигурациях Служба веб-публикации должна быть отключена.

### **Безопасность файловой системы**

Параметры безопасности, определяемые в настоящем разделе, применяются для операционной системы Microsoft® Windows® XP Professional, установленной на компьютерах, функционирующих в средах с высоким уровнем безопасности.

Параметры безопасности файловой системы могут быть изменены с использованием групповой политики. Устанавливаемые разрешения для файловой системы следует настраивать с помощью редактора групповой политики в следующем разделе пространства имен объекта групповой политики: Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Файловая система.

После настройки перечисленных ниже рекомендованных разрешений (см. таблицу А.2.8) следует удалить разрешения для файлов и папок в отношении группы «Все», поскольку в данную группу входят пользователи, не имеющие действительных учетных записей, и предоставить такие же разрешения локальной группе «Пользователи». Подобную стратегию можно использовать с целью ограничения доступа группе «Опытные пользователи», но в этом случае гораздо проще будет настроить и применить параметр «Группы с ограниченным доступом» с помощью групповой политики.

Таблица А.2.8– Параметры безопасности файловой системы

<b>Папка или файл</b>	<b>Группа пользователей</b>	<b>Устанавливаемые разрешения</b>	<b>Область применения</b>	<b>Метод наследования</b>
%AllUsersProfile% (Папка, содержащая атрибуты рабочего стола и профилей для всех пользователей, обычно C:\Documents and Settings\All Users)	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Распространять наследуемые разрешения на все подпапки и файлы
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	
%AllUsersProfile%\Application Data\Microsoft (Содержит данные документов приложений Microsoft)	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	
	Опытные пользователи	Весь перечень разрешений за исключением разрешений «Смена разрешений» и «Смена владельца»	Папка, ее подпапки и файлы	
%AllUsersProfile%\Application Data\Microsoft\Crypto\DSS\MachineKeys	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Заменять существующие разрешения для всех подпапок и файлов на наследуемые раз-



## Руководство по безопасной настройке и контролю сертифицированной версии

Папка или файл	Группа пользователей	Устанавливаемые разрешения	Область применения	Метод наследования
	SYSTEM	Полный доступ	Папка, подпапки и файлы	решения
	Пользователи	Содержание папки, Чтение атрибутов, Чтение дополнительных атрибутов, Создание файлов, Создание папок, Запись атрибутов, Запись дополнительных атрибутов, Чтение разрешений	Только эта папка	
%AllUsersProfile%\ Application Data\ Microsoft\Crypto\ RSA\MachineKeys	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Содержание папки, Чтение атрибутов, Чтение дополнительных атрибутов, Создание файлов, Создание папок, Запись атрибутов, Запись дополнительных атрибутов, Чтение разрешений	Только эта папка	

## Руководство по безопасной настройке и контролю сертифицированной версии

Папка или файл	Группа пользователей	Устанавливаемые разрешения	Область применения	Метод наследования
%AllUsersProfile%\Application Data\Microsoft\HTML Help	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	
	Опытные пользователи	Изменение	Папка, ее подпапки и файлы	
%AllUsersProfile%\Application Data\Microsoft\Media Index	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения
	SYSTEM	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Создание файлов, Создание папок, Запись атрибутов, Запись дополнительных атрибутов, Чтение разрешений	Только эта папка	
	Пользователи	Запись	Только подпапки и файлы	
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	

## Руководство по безопасной настройке и контролю сертифицированной версии

Папка или файл	Группа пользователей	Устанавливаемые разрешения	Область применения	Метод наследования
	Опытные пользователи	Весь перечень разрешений за исключением разрешений «Смена разрешений» и «Смена владельца»	Папка, ее подпапки и файлы	
%AllUsersProfile%\DRM	Игнорировать			Игнорировать
%SystemDrive% (Диск, на котором установлена операционная система Windows XP)	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Распространять наследуемые разрешения на все подпапки и файлы
	Создатель-владелец	Полный доступ	Только подпапки и файлы	
	Система	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	
%SystemDrive%\Documents and Settings (Папка, содержащая профили пользователей и профили по умолчанию)	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Распространять наследуемые разрешения на все подпапки и файлы
	Система	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	
	Опытные пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	

## Руководство по безопасной настройке и контролю сертифицированной версии

Папка или файл	Группа пользователей	Устанавливаемые разрешения	Область применения	Метод наследования
%SystemDrive%\Documents and Settings\Default User (Папка, содержащая используемые по умолчанию атрибуты рабочего стола и профиль пользователей, которые входят в систему впервые)	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения
	Система	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	
	Опытные пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	
%SystemRoot%\Installer	Администраторы	Полный доступ	Папка, ее подпапки и файлы	Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения
	Система	Полный доступ	Папка, ее подпапки и файлы	
	Пользователи	Чтение и выполнение	Папка, ее подпапки и файлы	
%SystemRoot%\Registration (Папка, содержащая файлы реестра балансировки нагрузки компонентов (CLB), которые читаются приложениями COM+)	Администраторы	Полный доступ	Папка и ее файлы	Заменять существующие разрешения для всех подпапок и файлов на наследуемые разрешения
	Система	Полный доступ	Папка и ее файлы	
	Пользователи	Чтение	Папка и ее файлы	

## **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® XP Professional 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 обеспечения 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® XP Professional проводится в следующей последовательности:

1. Провести экспертное обследование объекта информатизации.
2. Определить класс защищенности автоматизированной системы [1,2].

3. Установить операционную систему Microsoft® Windows® XP Professional 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. подраздел 3.4).

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);

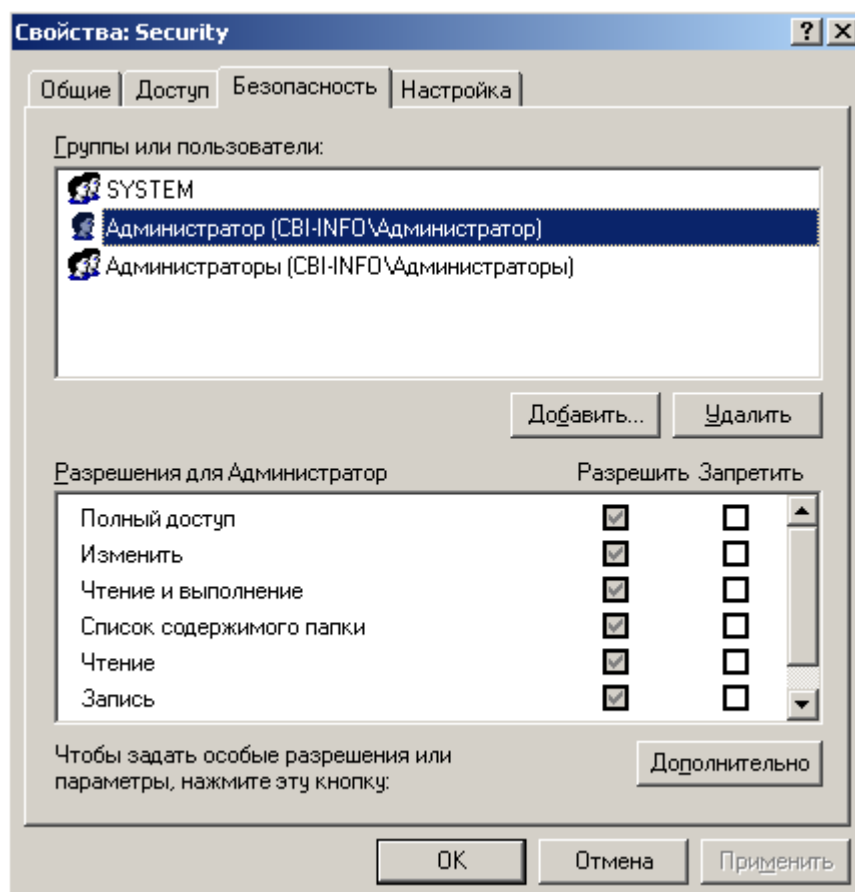


Рисунок Б.2.1

- 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):

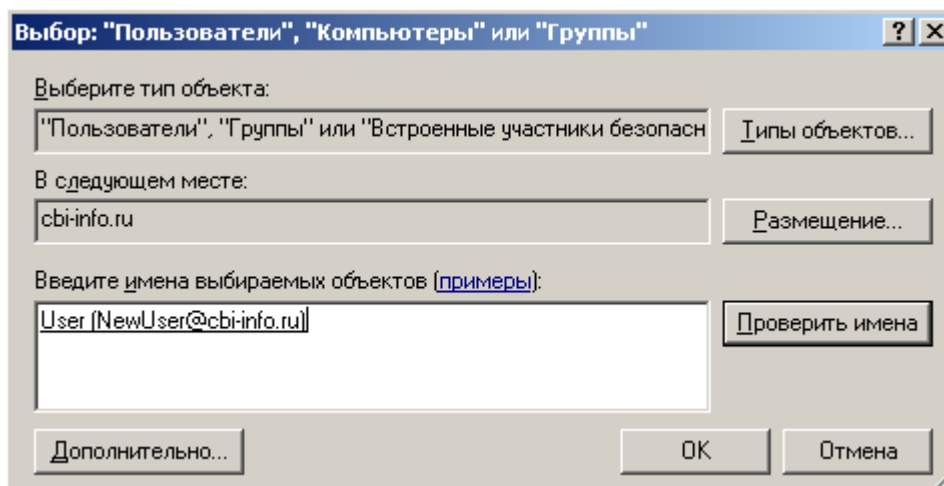


Рисунок Б.2.2

- 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).

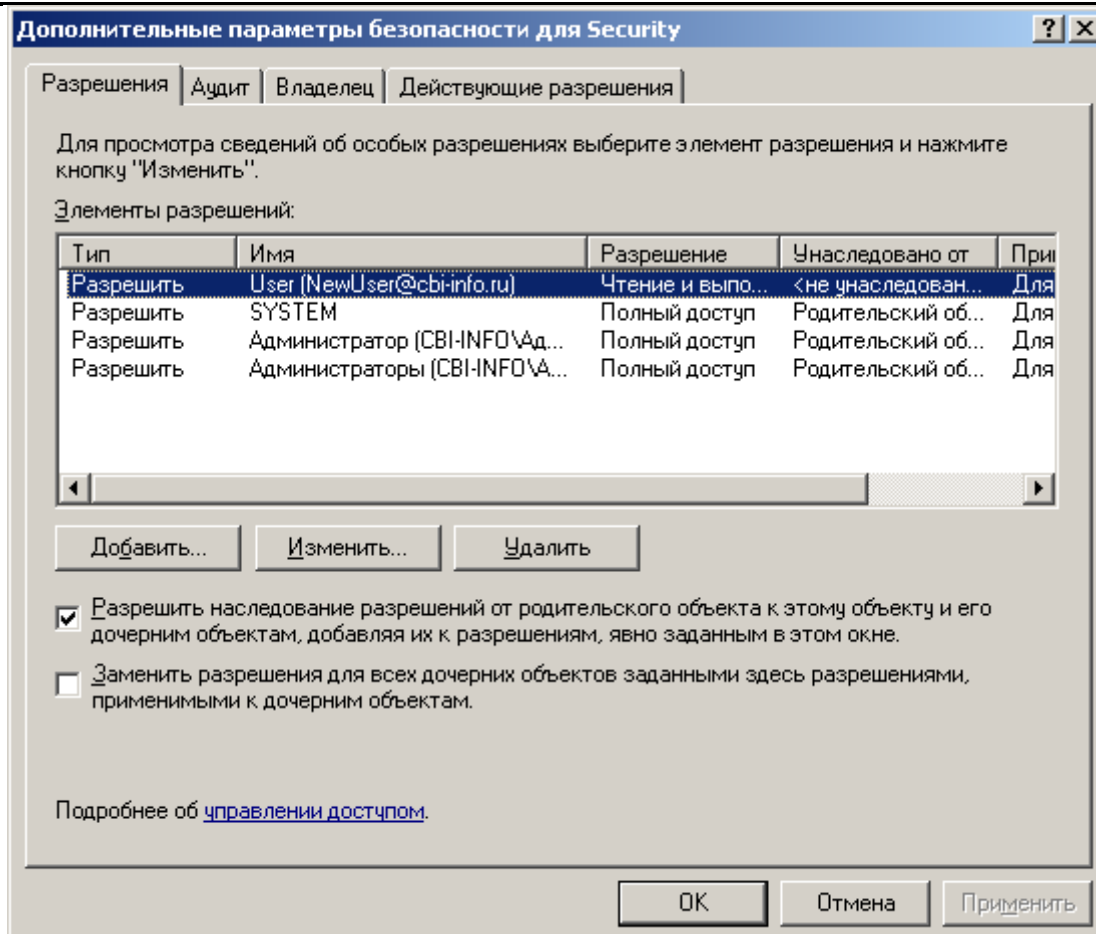
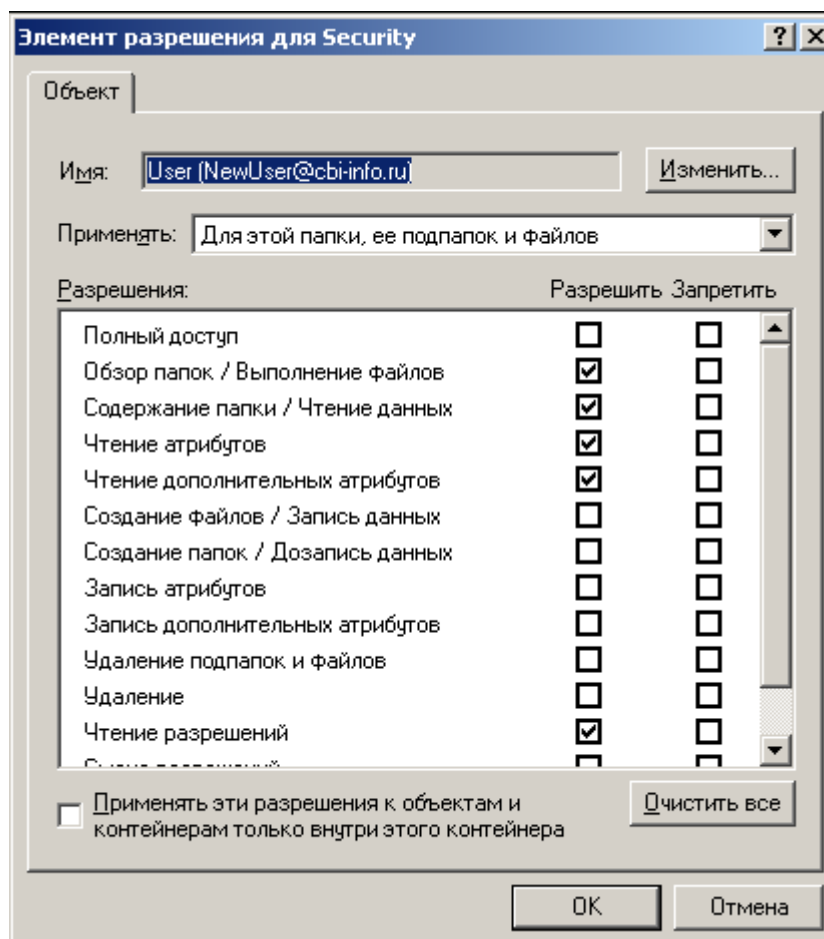


Рисунок Б.2.3



9. Провести проверку функционирования подсистемы управления доступом (механизмы идентификации, аутентификации и контроля доступа), подсистемы регистрации и учета, подсистемы обеспечения целостности.

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 ОС Microsoft® Windows® XP Professional », поставляемая на компакт-диске дополнительно к дистрибутиву операционной системы Microsoft® Windows® XP Professional ).

## **В.1 Рекомендованные значения параметров безопасности брандмауэра Windows**

Для обеспечения требуемого уровня безопасности с помощью редактора групповой политики необходимо настроить соответствующие параметры брандмауэра Windows в разделе пространства имен объекта групповой политики: Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения\Брандмауэр Windows (см. таблицу В.1.1).

Параметры, определяемые в разделе Конфигурация компьютера\Сеть\Сетевые подключения\Брандмауэр Windows\Профиль домена, управляют работой брандмауэра Windows при функционировании клиентского компьютера в вычислительной сети в составе домена Active Directory.

Параметры, определяемые в разделе Конфигурация компьютера\Сеть\Сетевые подключения\Брандмауэр Windows\Стандартный профиль, позволяют управлять работой брандмауэра Windows в случае, если клиентский компьютер не подключен к сети (является автономным) либо функционирует в вычислительной сети, но не входит в состав домена Active Directory, развернутого на ее базе.

Таблица В.1.1 – Параметры настройки брандмауэра Windows, используемые для обеспечения безопасности компьютеров под управлением операционной системы Microsoft® Windows® XP Professional

№ п/п	Параметры брандмауэра Windows	Рекомендуемые значения параметров брандмауэра Windows					
		Клиентский компьютер в конфигурации «High Security», являющийся членом домена Active Directory.	Клиентский компьютер в конфигурации «Enterprise», являющийся членом домена Active Directory.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене на базе Active Directory.	Автономный компьютер в конфигурации «High Security», функционирующий в домене на базе Active Directory.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене Windows NT 4.0 (или полностью автономно).	Автономный компьютер в конфигурации «High Security», функционирующий в домене Windows NT 4.0 (или полностью автономно).
1.	Брандмауэр Windows: Защитить все сетевые подключения	Включен	Включен	Включен	Включен	Включен	Включен
2.	Брандмауэр Windows: Не разрешать исключения	Не рекомендовано к использованию	Не рекомендовано к использованию	Рекомендовано к использованию	Рекомендовано к использованию	Рекомендовано к использованию	Рекомендовано к использованию
3.	Брандмауэр Windows: Задать исключения для программ	Рекомендовано к использованию	Рекомендовано к использованию	Рекомендовано к использованию	Рекомендовано к использованию	Рекомендовано к использованию	Рекомендовано к использованию
4.	Брандмауэр Windows: Разрешать локальные исключения для программ	Отключен	Не рекомендовано к использованию	Не рекомендовано к использованию	Отключен	Не рекомендовано к использованию	Отключен



№ п/п	Параметры брандмауэра Windows	Рекомендуемые значения параметров брандмауэра Windows					
		Клиентский компьютер в конфигурации «High Security», являющийся членом домена Active Directory.	Клиентский компьютер в конфигурации «Enterprise», являющийся членом домена Active Directory.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене на базе Active Directory.	Автономный компьютер в конфигурации «High Security», функционирующий в домене на базе Active Directory.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене Windows NT 4.0 (или полностью автономно).	Автономный компьютер в конфигурации «High Security», функционирующий в домене Windows NT 4.0 (или полностью автономно).
			пользованию	пользованию		пользованию	
5.	Брандмауэр Windows: Разрешать исключения для удаленного управления	Отключен	Рекомендовано к использованию	Отключен	Отключен	Отключен	Отключен
6.	Брандмауэр Windows: Разрешать исключения для общего доступа к файлам и принтерам	Отключен	Отключен	Отключен	Отключен	Отключен	Отключен
7.	Брандмауэр Windows: Разрешать исключения ICMP	Не рекомендовано к использованию	Не рекомендовано к использованию	Отключен	Отключен	Отключен	Отключен
8.	Брандмауэр Windows: Разрешать исключения для удаленного рабочего стола	Рекомендовано к использованию	Рекомендовано к использованию	Включен	Включен	Включен	Включен

№ п/п	Параметры брандмауэра Windows	Рекомендуемые значения параметров брандмауэра Windows					
		Клиентский компьютер в конфигурации «High Security», являющийся членом домена Active Directory.	Клиентский компьютер в конфигурации «Enterprise», являющийся членом домена Active Directory.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене на базе Active Directory.	Автономный компьютер в конфигурации «High Security», функционирующий в домене на базе Active Directory.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене Windows NT 4.0 (или полностью автономно).	Автономный компьютер в конфигурации «High Security», функционирующий в домене Windows NT 4.0 (или полностью автономно).
9.	Брандмауэр Windows: Разрешать исключения для UPnP-инфраструктуры	Не рекомендовано к использованию	Не рекомендовано к использованию	Отключен	Отключен	Отключен	Отключен
10.	Брандмауэр Windows: Запретить уведомления	Не рекомендовано к использованию	Не рекомендовано к использованию	Не рекомендовано к использованию	Не рекомендовано к использованию	Не рекомендовано к использованию	Не рекомендовано к использованию
11.	Брандмауэр Windows: Разрешать ведение журнала	Включен	Включен	Включен	Включен	Включен	Включен
12.	Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковебательные запросы	Включен	Включен	Включен	Включен	Включен	Включен

№ п/п	Параметры брандмауэра Windows	Рекомендуемые значения параметров брандмауэра Windows					
		Клиентский компьютер в конфигурации «High Security», являющийся членом домена Active Directory.	Клиентский компьютер в конфигурации «Enterprise», являющийся членом домена Active Directory.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене на базе Active Directory.	Автономный компьютер в конфигурации «High Security», функционирующий в домене на базе Active Directory.	Автономный компьютер в конфигурации «Enterprise», функционирующий в домене Windows NT 4.0 (или полностью автономно).	Автономный компьютер в конфигурации «High Security», функционирующий в домене Windows NT 4.0 (или полностью автономно).
13.	Брандмауэр Windows: Задать исключения для портов	Не рекомендовано к использованию	Не рекомендовано к использованию	Не рекомендовано к использованию	Не рекомендовано к использованию	Не рекомендовано к использованию	Не рекомендовано к использованию
14.	Брандмауэр Windows: Разрешать локальные исключения для портов	Отключен	Отключен	Отключен	Отключен	Отключен	Отключен

Параметр «Брандмауэр Windows: Защитить все сетевые подключения» включает брандмауэр Windows для всех сетевых подключений клиентского компьютера, заменяя при этом брандмауэр подключения к Интернету (Internet Connection Firewall) на компьютерах, работающих под управлением ОС Microsoft® Windows® XP Professional . При включении указанной политики параметр «Запретить использование брандмауэра подключения к Интернету в сети DNS-домена» в папке Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения игнорируется.

В обоих вариантах рассматриваемых конфигураций указанный параметр должен иметь значение «Включен». Это позволит защитить компьютер от возможных сетевых атак и исключить возможность отключения брандмауэра Windows локальными администраторами компьютеров.

Параметр «Брандмауэр Windows: Не разрешать исключения» указывает на то, что брандмауэр Windows будет блокировать любые незапрашиваемые входящие сообщения. Указанная политика перекрывает все другие политики брандмауэра Windows, которые разрешают такие сообщения.

В обоих вариантах рассматриваемых конфигураций при условии, что клиентский компьютер является членом домена Active Directory, использовать данную политику не рекомендуется. Это позволит брандмауэру Windows применять другие политики, которые могут разрешать получение незапрашиваемых входящих сообщений, поскольку в сети могут использоваться приложения, требующие получения такого типа сообщений для своего нормального функционирования. В отдельных случаях указанная политика может быть отключена с целью исключения возможности ее включения локальными администраторами компьютеров, что приведет к блокированию всех санкционированных и несанкционированных попыток подключения к клиентским компьютерам.

В случае с автономным компьютером для обеспечения его большей защищенности рекомендуется использовать данную политику (при условии, что не планируется использовать другие политики брандмауэра Windows). Это позволит блокировать любые незапрашиваемые входящие сообщения и перекрыть все другие политики брандмауэра Windows.

Параметр «Брандмауэр Windows: Задать исключения для программ» позволяет определить список исключений для программ, заданных групповой политикой. Брандмауэр Windows использует два списка исключений для программ: первый

определяется параметрами групповой политики, второй – непосредственно через панель управления посредством локальной настройки брандмауэра Windows.

При добавлении программы к списку исключений, она сможет получать незапрашиваемые входящие сообщения по любому из портов, которые она открывает с помощью брандмауэра Windows, даже если этот порт заблокирован с помощью другой политики, например, политики «Брандмауэр Windows: Задать исключения для портов».

Если параметру состояния строки определения из списка исключения для программ присвоено значение «disabled», брандмауэр Windows игнорирует любые запросы на открытие порта и игнорирует другие строки определения, которые устанавливают значение параметра состояния программы равным «enabled». Таким образом, если состояние установлено равным «disabled», локальные администраторы не могут разрешить программе запрашивать брандмауэр Windows об открытии дополнительного порта. Однако, в ряде случаев программа сможет получить незапрашиваемые входящие сообщения через порт, несмотря на то, что значение параметра состояния программы равным «disabled». Это возможно при условии, что требуемый порт открыт другой политикой брандмауэра Windows.

Для обоих вариантов рассматриваемых конфигурации указанная политика рекомендуется к использованию, что требует определения списка исключений для программ, которые могут получать незапрашиваемые входящие сообщения по любому из портов. При этом область действия указанной политики должна распространяться только на клиентские компьютеры вычислительной сети (подсети), в составе которой функционирует целевой компьютер, или на клиентские компьютеры иной доверенной вычислительной сети (подсети).

Параметр «Брандмауэр Windows: Разрешать локальные исключения для программ» позволяет локальным администраторам компьютеров осуществлять настройку брандмауэра Windows в части задания списка локальных исключений для программ.

В конфигурации «High Security» указанная политика должна быть отключена, что позволит избежать несанкционированного задания локальными администраторами компьютеров списков исключения для программ. В конфигурации «Enterprise» указанную политику использовать также не рекомендуется. Однако, при функционировании клиентского компьютера в данной конфигурации может возникнуть необходимость задания администратором списка локальных исключений для программ в соответствии с

имеющимися потребностями, которые не были учтены на этапе проектирования и внедрения групповой политики. Эти потребности, прежде всего, связаны с установкой нового программного обеспечения или с использованием приложением нестандартных портов. В этих случаях, администратором безопасности может быть разрешены локальные исключения для программ.

Параметр «Брандмауэр Windows: Разрешать исключения для удаленного управления» определяет возможность удаленного управления целевым компьютером с помощью таких средств администрирования, как консоль управления Microsoft (MMC) и инструментария управления Windows. Для этого брандмауэр Windows открывает порты 135 протокола UDP и 445 протокола TCP. Системные службы Windows обычно используют эти порты для поддержания связи с использованием механизма RPC (remote procedure calls) и DCOM (Distributed Component Object Model). Данная политика также разрешает службам `svchost.exe` и `lsass.exe` получение незапрашиваемых входящих сообщений, что позволяет им открывать дополнительные, динамически назначаемые порты, обычно в диапазоне от 1024 до 1034.

Поскольку злоумышленники часто пытаются атаковать компьютеры с помощью эксплойтов (программа, использующая известную уязвимость для организации различного типа атак на компьютер), использующих уязвимости RPC и DCOM, в средах с высокими требованиями к безопасности и на автономных компьютерах рекомендуется не включать данную политику. Поэтому в случае если клиентский компьютер функционирует в конфигурации «High Security» или является автономным указанную политику рекомендуется отключить.

При функционировании клиентского компьютера в конфигурации «Enterprise» и необходимости удаленного управления клиентскими компьютерами указанную политику рекомендуется включить. При этом в данной конфигурации область ее действия должна охватывать диапазон действительных IP-адресов собственной или доверенной вычислительной сети (подсети). Кроме того, указанная политика должна разрешать незапрашиваемые входящие сообщения, ассоциируемые с удаленным управлением, только от конкретных клиентских компьютеров, используемых для удаленного управления вычислительной сетью (подсетью).

Параметр «Брандмауэр Windows: Разрешать исключения для общего доступа к файлам и принтерам» определяет возможность предоставления общего доступа к файлам и принтерам. Для этого брандмауэр Windows открывает порты 137 и 138 протокола UDP и порты 139 и 445 протокола TCP. Если указанная политика включена,

брандмауэр Windows открывает данные порты и разрешает клиентскому компьютеру получать задания печати и запросы на общий доступ к файлам.

Если эта политика отключена, брандмауэр Windows блокирует указанные порты, что не позволяет компьютеру предоставить общий доступ к файлам и принтерам. Если администратор попытается открыть какой-нибудь из этих портов путем добавления его в список исключений, брандмауэр Windows не откроет требуемый порт.

В обоих вариантах рассматриваемых конфигураций при функционировании клиентских компьютеров в составе домена Active Directory или в качестве автономных рабочих станций указанная политика должна быть отключена, поскольку роли файлового сервера и сервера печати не типичны для клиентских компьютеров под управлением ОС Microsoft® Windows® XP Professional и должны реализовываться выделенными компьютерами, предназначенными именно для этих целей.

В случае необходимости использования клиентских компьютеров в качестве сервера печати или файлового сервера область действия данной политики должна охватывать диапазон действительных IP-адресов собственной или доверенной вычислительной сети (подсети). При этом необходимо указать действительные IP-адреса конкретных клиентских компьютеров, от которых разрешается получать задания печати и запросы на общий доступ к файлам.

Параметр «Брандмауэр Windows: Разрешать исключения ICMP» определяет разрешенный брандмауэром Windows набор сообщений ICMP (Internet Control Message Protocol), используемых служебными программами для определения состояния других компьютеров.

В обоих вариантах рассматриваемых конфигураций безопасности рекомендуется отключить данную политику, что позволит блокировать все незапрашиваемые входящие типы сообщений ICMP и перечисленные в списке исходящие типы сообщений ICMP. При этом если какая-либо из политик открывает порт 445 протокола TCP, брандмауэр Windows разрешает входящие запросы эха, даже если политика «Брандмауэр Windows: Разрешать исключения ICMP» блокирует их.

В случае использования на компьютере приложений, требующих для своего правильного функционирования обмен заданными типами сообщений ICMP, администратором должна быть осуществлена соответствующая настройка данной политики, которая будет отражать указанные исключения.

Параметр «Брандмауэр Windows: Разрешать исключения для удаленного рабочего стола» позволяет компьютеру получать запросы на запуск

удаленного рабочего стола. Для этого брандмауэр Windows открывает порт 3389 протокола TCP.

Если эта политика включена, брандмауэр Windows открывает этот порт, для того чтобы компьютер мог получать запросы на запуск удаленного рабочего стола. Если эта политика отключена, брандмауэр Windows блокирует этот порт, и компьютер не сможет получать запросы на запуск удаленного рабочего стола даже в том случае, если указанный порт будет добавлен в список исключений для портов.

Для обеспечения расширенных возможностей управления вычислительной средой в обоих вариантах рассматриваемых конфигураций данную политику рекомендуется включить. Область действия данной политики должна охватывать диапазон действительных IP-адресов собственной или доверенной вычислительной сети (подсети). При этом по возможности удаленные незапрашиваемые входящие подключения к рабочему столу должны быть разрешены только с конкретных клиентских компьютеров.

Параметр «Брандмауэр Windows: Разрешать исключения для UPnP-инфраструктуры» разрешает компьютеру получать незапрашиваемые сообщения PnP, отправленные сетевыми устройствами, такими как маршрутизаторы со встроенными брандмауэрами. Для этого брандмауэр Windows открывает порт 2869 протокола TCP и порт 1900 протокола UDP.

Если эта политика включена, брандмауэр Windows открывает эти порты, для того чтобы компьютер мог получать сообщения PnP. В противном случае, брандмауэр Windows блокирует эти порты, что не позволяет компьютеру получать сообщения PnP. При этом если администратор попытается открыть порты путем добавления их в список исключений для локальных портов, брандмауэр Windows не откроет указанные порты.

В обоих вариантах рассматриваемых конфигураций данную политику рекомендуется отключить.

Параметр «Брандмауэр Windows: Запретить уведомления» определяет возможность отображения брандмауэром Windows уведомления пользователю о том, что программа запрашивает у брандмауэра добавить ее в список исключений. Данная ситуация возникает в случае, когда программа пытается открыть порт, не разрешенный текущей политикой безопасности брандмауэра Windows.

Если данная политика будет разрешена, то брандмауэр Windows будет блокировать все попытки уведомлений. В противном случае брандмауэр Windows будет разрешать отображение уведомлений.



Обычно пользователям не разрешено добавлять программы или порты в списки исключений брандмауэра Windows, поэтому указанные уведомления будут носить для них информативный характер. В таких случаях данная политика должна быть разрешена. В средах, где пользователи (администраторы) обладают полномочиями по управлению списками исключений для программ и портов, данная политика должна быть запрещена.

Параметр «Брандмауэр Windows: Разрешать ведение журнала» определяет возможность записи брандмауэром Windows информации о получаемых им входящих сообщениях. Благодаря фиксации информации о входящих сообщениях, которые были заблокированы (отброшены) брандмауэром, и информации об успешных входящих или исходящих подключениях, в случае возникновения нарушений, связанных с безопасностью, администратор безопасности сможет идентифицировать сущность, источник и другие параметры нарушений.

При включении указанной политики следует указать, какую информацию следует записывать в журнал безопасности брандмауэра Windows, а также имя, расположение и максимальный размер файла журнала безопасности.

В обоих вариантах рассматриваемых конфигураций безопасности рекомендуется задавать такое значение максимального размера файла журнала безопасности, при котором будет достаточно места для записи событий, связанных с функционированием брандмауэра Windows, при этом он не должен занимать слишком много дискового пространства. Поэтому в обеих конфигурациях для данного параметра рекомендуется значение 10240 Кб. Кроме того, при задании политики необходимо указать, какие категории событий аудита брандмауэру следует отслеживать. Рекомендуется записывать информацию о входящих сообщениях, которые были заблокированы (отброшены), и информацию об успешных входящих или исходящих подключениях.

Параметр «Брандмауэр Windows: Запретить одноадресные ответы на многоадресные или широковещательные запросы» запрещает компьютеру получать одноадресные (unicast) ответы на свои многоадресные (multicast) или широковещательные (broadcast) сообщения.

Если эта политика включена, и компьютер отправляет многоадресные или широковещательные сообщения другим компьютерам, брандмауэр Windows блокирует одноадресные ответы, отправляемые ими. Если эта политика отключена или не задана, и компьютер отправляет многоадресные или широковещательные сообщения другим компьютерам, брандмауэр Windows ожидает в течение трех секунд получения одноадресных ответов от этих компьютеров, а затем блокирует все отправленные позже ответы.

Обычно одноадресные ответы на многоадресные или широковещательные сообщения служат признаком атак типа «отказ в обслуживании» или попыток злоумышленника определить включен клиентский компьютер или нет. Поэтому в обоих вариантах рассматриваемых конфигураций безопасности данную политику рекомендуется включить. Однако при включении указанной политики нужно учитывать, что она может оказывать воздействие на сообщения NetBIOS, которые служат для обнаружения конфликтов имен в сети.

Параметр «Брандмауэр Windows: Задать исключения для портов» позволяет просматривать и изменять список исключений для портов, заданных групповой политикой. Брандмауэр Windows использует два списка исключений для портов: первый определяется параметрами групповой политики, второй – непосредственно через панель управления посредством локальной настройки брандмауэра Windows.

При добавлении порта к списку исключений, клиентский компьютер сможет получать незапрашиваемые входящие подключения на указанный порт TCP или UDP, который он открывает с помощью брандмауэра Windows.

Если параметру состояния строки определения из списка исключения для портов присвоено значение «disabled», брандмауэр Windows игнорирует любые запросы на открытие порта и игнорирует другие строки определения, которые устанавливают значение параметра состояния порта равным «enabled», т.е. перекрывает все другие значения. Таким образом, если состояние установлено равным «disabled», локальные администраторы не могут использовать брандмауэр Windows для открытия порта. Однако в ряде случаев клиентский компьютер сможет получать незапрашиваемые входящие подключения на указанный порт TCP или UDP, несмотря на то, что значение параметра состояния порта установлено равным «disabled». Это возможно при условии, что требуемый порт открыт другой политикой брандмауэра Windows либо программой из списка исключений.

Включение данной политики допускается при условии использования на компьютере нестандартных приложений при условии невозможности использования списка исключений для программ. Исключения для программ позволяет брандмауэру Windows получать запросы на незапрашиваемые входящие подключения только в том случае, если программа запущена. В свою очередь задание исключений для портов делает их открытыми все время. Поэтому в обоих вариантах рассматриваемых конфигураций безопасности данную политику рекомендуется отключить.

Параметр «Брандмауэр Windows: Разрешать локальные исключения для портов» позволяет локальным администраторам компьютера осуществлять настройку брандмауэра Windows в части задания списка локальных исключений для портов.

В обеих конфигурация безопасности указанная политика должна быть отключена, что позволит исключить возможность самостоятельного задания локальными администраторами компьютеров списков исключения для портов и, таким образом, избежать несанкционированных незапрашиваемых входящих подключений.