ЦБИ-сервис

ОФИСНЫЙ ПРОГРАММНЫЙ КОМПЛЕКС MICROSOFT® OFFICE ПРОФЕССИОНАЛЬНЫЙ ВЫПУСК 2003

Включающий пакет обновлений Service Pack 3

РУССКАЯ ВЕРСИЯ

РУКОВОДСТВО ПО БЕЗОПАСНОЙ НАСТРОЙКЕ И КОНТРОЛЮ СЕРТИФИЦИРОВАННОЙ ВЕРСИИ

2008

СОДЕРЖАНИЕ

1 Введение 4

2 Последовательность действий по настройке сертифицированной версии офисного программного комплекса Microsoft® Office 2003 6

2.1 Общие указания по настройке параметров безопасности сертифицированной версии офисного программного комплекса Microsoft® Office 2003 6

2.2 Порядок настройки Microsoft® Office 2003, установленного на клиентском компьютере в составе домена Active Directory, в соответствии с конфигурациями «Enterprise» и «High Security» 8

2.2.1 Общие указания 8

2.2.2 Порядок применения групповой политики для компьютеров, являющихся членами домена Active Directory 9

2.2.3 Используемые административные шаблоны 10

2.2.4 Порядок добавления административного шаблона 10

2.3 Порядок настройки Microsoft® Office 2003, установленного на автономном клиентском компьютере, в соответствии с конфигурациями «Enterprise» и «High Security» 16

2.3.1 Используемые административные шаблоны 16

2.3.2 Порядок добавления административного шаблона 17

2.4 Рекомендуемые параметры безопасности Microsoft® Office 2003 для конфигураций «Enterprise» и «High Security» 21

2.5 Порядок копирования и контрольного суммирования пакета обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003 26

2.6 Порядок установки пакета обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003 28

2.7 Порядок копирования и установки наборов исправлений безопасности для офисного программного комплекса Microsoft® Office 2003 33

3 Последовательность действий по контролю сертифицированной версии Microsoft® Office 2003 35

© ЗАО «ЦБИ-сервис», 2008

3.1 Контроль маркирования сертифицированной версии офисного программного комплекса Microsoft® Office 2003 35

3.2 Автоматизированный контроль сертифицированной версии офисного программного комплекса Microsoft® Office 2003 35

© ЗАО «ЦБИ-сервис», 2008

1 Введение

Настоящий документ содержит рекомендации по настройке и контролю механизмов защиты офисного программного комплекса «Microsoft® Office, Профессиональный выпуск 2003, Русская редакция» (далее Microsoft® Office 2003) при организации обработки конфиденциальной информации на объекте информатизации.

Руководство предназначено для настройки механизмов защиты офисного программного комплекса Microsoft® Office 2003 в соответствиисоследующими конфигурациями безопасности, в которых данное изделие было сертифицировано:

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

При этом обе конфигурации безопасности не зависят от наличия инфраструктуры домена Active Directory, предполагая возможность централизованного и децентрализованного управления параметрами безопасности офисного программного комплекса Microsoft® Office 2003. Отличие конфигурации «High Security» по сравнению с конфигурацией «Enterprise заключается в использовании для офисного программного комплекса Microsoft® Office 2003» более ограничивающей политики безопасности и усиленных настроек безопасности.

Офисный программный комплекс Microsoft® Office 2003 может быть установлен на клиентском компьютере, функционирующем под управлением операционной системы Microsoft® Windows® XP Professional, как в составе локальной вычислительной сети, так и автономно (когда компьютер не включен в домен Active Directory или является членом домена Microsoft Windows NT® 4.0). Режим функционирования клиентского компьютера определяет порядок управления его параметрами безопасности (централизованное или децентрализованное управление политиками безопасности) и не влияет на устанавливаемые
для них значения. При функционировании клиентского компьютера в составе локальной вычислительной сети, в которой развернута инфраструктура службы каталогов Microsoft® Active Directory™ на базе операционной системы семейства Microsoft® Windows Server 2003™, управление параметрами безопасности офисного программного комплекса Microsoft® Office 2003 будет осуществляться с использованием административных шаблонов, добавляемых к соответствующим объектам групповой политики (ОГП), базируемым на

© ЗАО «ЦБИ-сервис», 2008

Active Directory. В противном случае, управление параметрами безопасности данного клиентского компьютера будет осуществляться посредством локального ОГП - локальной политики безопасности.

© ЗАО «ЦБИ-сервис», 2008

Таким образом, исходя из рассмотренных выше режимов функционирования (не оказывающих непосредственного влияния на определяемые с использованием административных шаблонов значения параметров безопасности Microsoft® Office 2003) и конфигураций безопасности, можно выделить следующие варианты функционирования офисного программного комплекса Microsoft® Office 2003 (см. таблицу 1.1).

Таблица 1.1 – Варианты функционирования офисного программного комплекса Microsoft® Office 2003

№ п/п	Варианты функционирования офисного программного комплекса
1.	Офисный программный комплекс Microsoft® Office 2003 в конфигурации «High Security», установленный на клиентском компьютере в составе домена Active Directory.
2.	Офисный программный комплекс Microsoft® Office 2003 в конфигурации «Enterprise», установленный на клиентском компьютере в составе домена Active Directory.
3.	Офисный программный комплекс Microsoft® Office 2003 в конфигурации «High Security», установленный на автономном компьютере.
4.	Офисный программный комплекс Microsoft® Office 2003 в конфигурации «Enterprise», установленный на автономном компьютере.

2 Последовательность действий по настройке сертифицированной версии офисного программного комплекса Microsoft® Office 2003

2.1 Общие указания по настройке параметров безопасности сертифицированной версии офисного программного комплекса Microsoft® Office 2003

Офисный программный комплекс Microsoft® Office 2003 сертифицирован в конфигурациях «Enterprise» и «High Security» для вариантов функционирования, перечисленных в таблице 1.1.

Для реализации политики безопасности, соответствующей сертифицированным конфигурациям «Enterprise» или «High Security», администратору эксплуатирующей организации необходимо выполнить настройку требуемых параметров безопасности Microsoft® Office 2003. При этом настройка параметров безопасности с использованием групповой политики может быть осуществлена только после добавления в окне оснастки консоли управления, используемой для редактирования объектов групповой политики (оснастки «Групповая политика» или «Редактор объектов групповой политики»), соответствующего административного шаблона, что обеспечивает создание пользовательского интерфейса для редактирование ключей реестра, соответствующих каждому настраиваемому параметру безопасности офисного программного комплекса Microsoft® Office 2003. Таким образом, размещенные на компакт-диске, входящем в комплект поставки сертифицированной версии офисного программного комплекса Microsoft® Office 2003, административные шаблоны (файлы с расширением `*.adm`) обеспечивают только отображение относящихся к Microsoft® Office 2003 параметров безопасности в дереве имен объектов оснастки (add-in) консоли управления «Групповая политика» (оснастки «Редактор объектов групповой политики» в среде Active Directory™). В файле административного шаблона содержаться следующие сведения:

- размещение параметров реестра, соответствующих каждому настраиваемому параметру;
- величина параметров или ограничений, связанных с каждым настраиваемым параметром;
- значение по умолчанию для параметров.

Примечание: Административные шаблоны не содержат предопределенные в соответствии с сертифицированными конфигурациями безопасности значения параметров безопасности. Они обеспечивают только интерфейс для редактирования тех

записей реестра, которые явно указаны в файле административного шаблона `*.adm`.

Использование административных шаблонов позволяет упростить выполнение задач администрирования, так как единую конфигурацию безопасности можно настроить сразу для всех офисных программных комплексов Microsoft® Office 2003, установленных на разных клиентских компьютерах, функционирующих в среде Active Directory™. При этом заданные настройки параметров безопасности Microsoft® Office 2003 будут затрагивать всех пользователей, работающих с офисным программным комплексом на данных клиентских компьютерах.

По умолчанию, на клиентских компьютерах под управлением операционной системы Microsoft® Windows® XP Professional для хранения файлов административных шаблонов используется папка `%SystemRoot%\inf\`. Во избежание возникновения проблем с управлением версиями административных шаблонов, необходимо определить файловый ресурс для хранения оригинала шаблонов. Оптимальной является практика, когда изменения всегда вносятся в одну и ту же копию административных шаблонов. Резервную копию административных шаблонов политики необходимо хранить в защищенном от несанкционированного доступа месте, доступ к которому предоставляется только администраторам.

Настройку параметров безопасности офисного программного комплекса Microsoft® Office 2003 в соответствии с конфигурациями «Enterprise» или «High Security» необходимо осуществлять через использование механизма 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 заданную конфигурацию безопасности, описанную с помощью соответствующих административных шаблонов. Альтернативой централизованному применению групповой политики является настройка каждого используемого в организации офисного программного комплекса Microsoft® Office 2003 вручную. Таким образом, в зависимости от режимов функционирования клиентского компьютера (в автономном режиме или в составе домена Active Directory) настройку параметров безопасности Microsoft® Office 2003 необходимо осуществлять либо непосредственно на клиентских компьютерах с использованием локального ОГП, либо на контроллере домена с использованием нелокальных ОГП, базируемых на Active Directory™.

Рекомендованные для каждой конфигурации значения параметров позволят

обеспечить безопасную обработку информации с использованием офисного программного комплекса Microsoft® Office 2003, а также создать среду, защищенную от большинства современных угроз безопасности.

2.2 Порядок настройки Microsoft® Office 2003, установленного на клиентском компьютере в составе домена Active Directory, в соответствии с конфигурациями «Enterprise» и «High Security»

2.2.1 Общие указания

Применению групповой политики, содержащей параметры безопасности, соответствующие сертифицированной конфигурации офисного программного комплекса Microsoft® Office 2003, должно предшествовать выполнение ряда подготовительных операций, а именно:

- создание организационного подразделения (ОП - это контейнер, используемый для объединения объектов домена Active Directory™ в логические административные группы), содержащего учетные записи клиентских компьютеров с установленным офисным программным комплексом Microsoft® Office 2003. При этом должно быть осуществлено разделение клиентских компьютеров по организационным подразделения в соответствии с настраиваемыми для Microsoft® Office 2003 конфигурациями безопасности (например, ОП «Enterprise XP Client» и ОП «High Security XP Client»);
- создание объекта групповой политики (ОГП);
- осуществление привязки созданного ОГП к соответствующему организационному подразделению (см. рисунок 2.1);
- добавление в окне редактора объекта групповой политики административного шаблона, содержащего сведения о настраиваемых в соответствии с сертифицированной конфигурацией параметрах безопасности Microsoft® Office 2003;
- задание требуемых значений параметров безопасности в соответствии с сертифицированными конфигурациями.

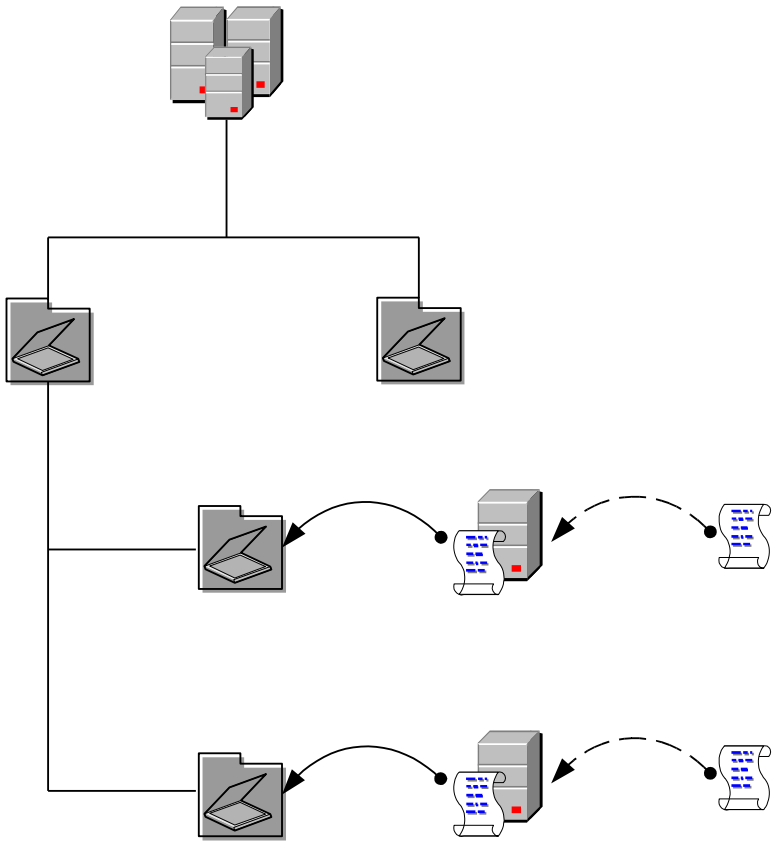


Рисунок 2.1 – Иерархия ОП и применяемых ОГП

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

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

1. **Local group policy** – локальная политика;
2. **Site-level group policies** – групповые политики, применяемая на уровне сайта (область вычислительной сети, обеспечивающей объединение контроллеров домена высокоскоростными и надежными каналами связи);
3. **Domain-level group policies** - групповые политики, применяемая на уровне домена Active Directory;
4. **OU-level group policies** – групповые политики уровня организационного подразделения.

2.2.3 Используемые административные шаблоны

Для автоматической настройки параметров безопасности используемых в организации офисных программных комплексов Microsoft® Office 2003, установленных на клиентских компьютерах, являющихся членами домена Active Directory™, необходимо создать объект групповой политики и осуществить его привязку к соответствующему организационному подразделению, содержащему учетные записи клиентских компьютеров, офисные программные комплексы которых должны быть настроены в соответствии с конфигурациями «Enterprise» или «High Security». Далее, обеспечить отображение относящихся к Microsoft® Office 2003 параметров безопасности в дереве имен объектов оснастки консоли управления «Редактор объектов групповой политики». Для этого в окне редактора объекта групповой политики следует добавить административный шаблон `Office11.adm`.

2.2.4 Порядок добавления административного шаблона

Добавление административного шаблона `Office11.adm`, предоставляющего интерфейс настройки параметров безопасности различных компонентов, входящих в состав сертифицированной версии офисного программного комплекса Microsoft® Office 2003, необходимо осуществлять с использованием редактора соответствующего объекта групповой политики (в частности, в данном руководстве будут использоваться ссылки на ОГП «Enterprise Client Office Policy» и ОГП «High Security Office Policy»). Чтобы добавить административный шаблон `Office11.adm` 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 2.2).

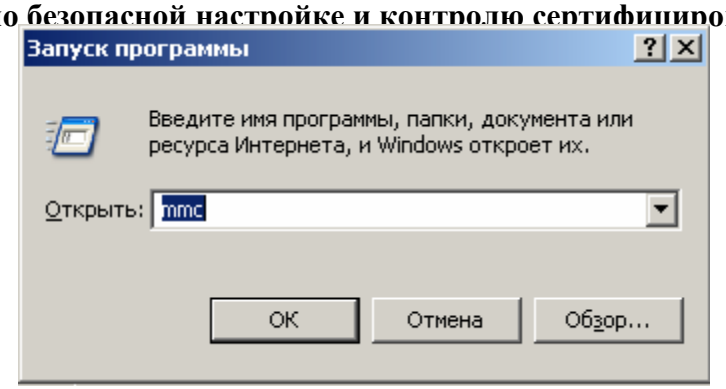

Запуск программы
Введите имя программы, папки, документа или ресурса Интернета, и Windows откроет их.
Открыть:
mmc
OK
Отмена
Обзор...

Рисунок 2.2.

2. В окне консоли управления MMC (MMC – Microsoft Management Console) через пункт меню «Добавить или удалить оснастку» добавить оснастку «Редактор объектов групповой политики» и выбрать требуемый объект групповой политики (например, «Enterprise Client Office Policy» либо ОГП «High Security Client Office Policy», если Microsoft® Office 2003 будет настраиваться в соответствии с конфигурацией «High Security») (см. рисунок 2.3-2.4).

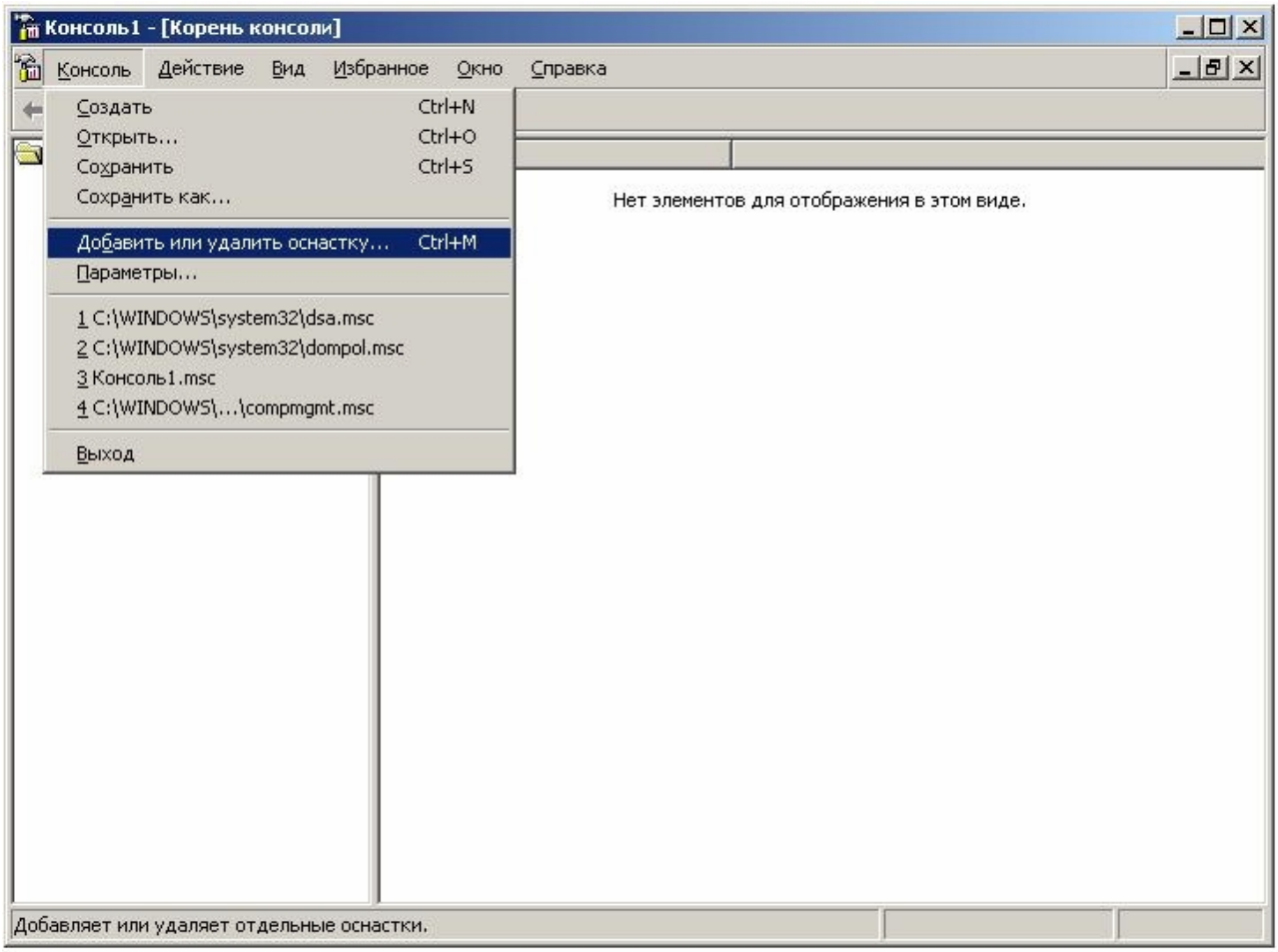


Рисунок 2.3

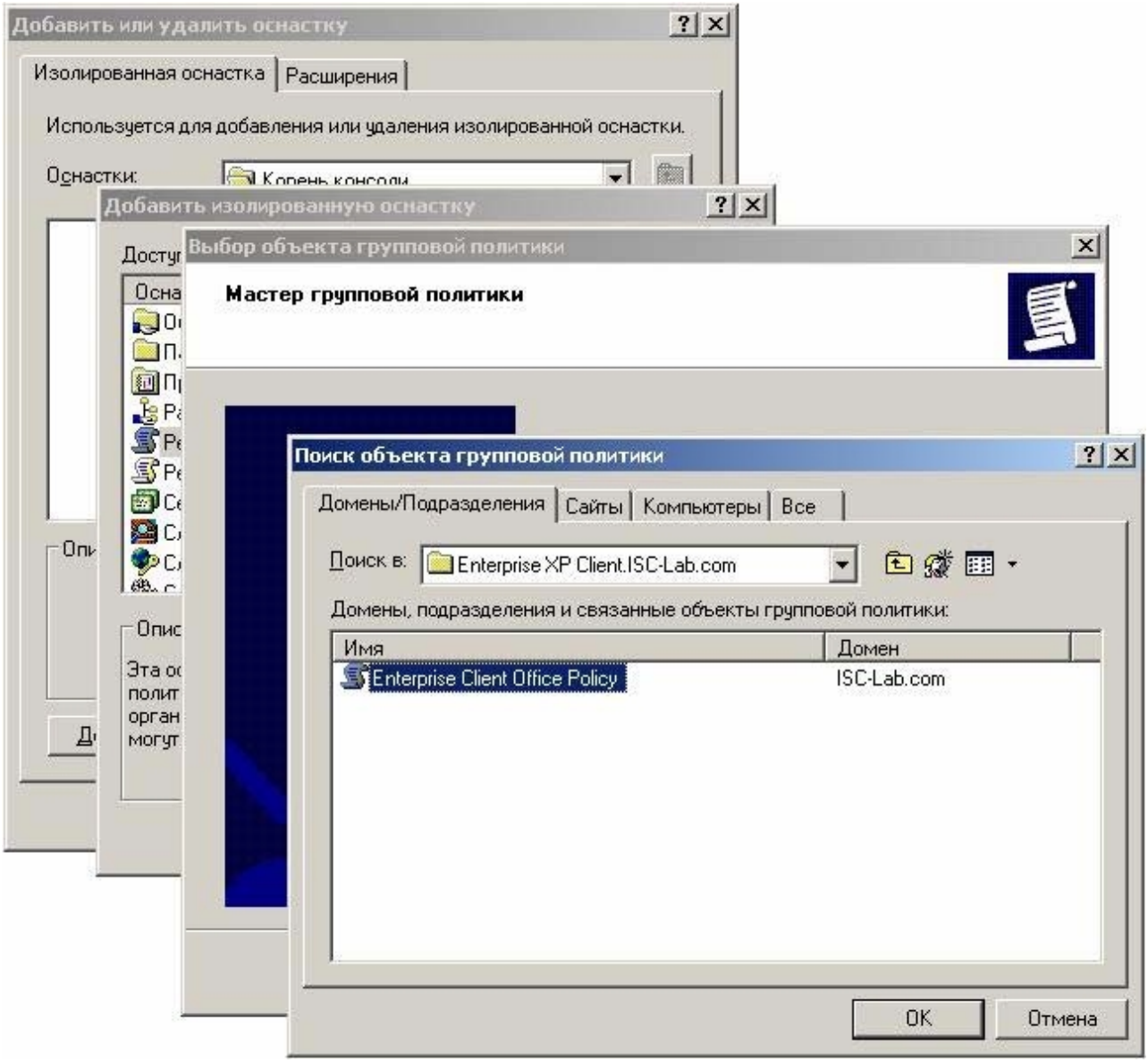


Рисунок 2.4

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.

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

4. Правой кнопкой мыши нажать на элемент «Административные шаблоны» и в появившемся окне контекстного меню выбрать команду «Добавление и удаление шаблонов» (см. рисунок 2.5).

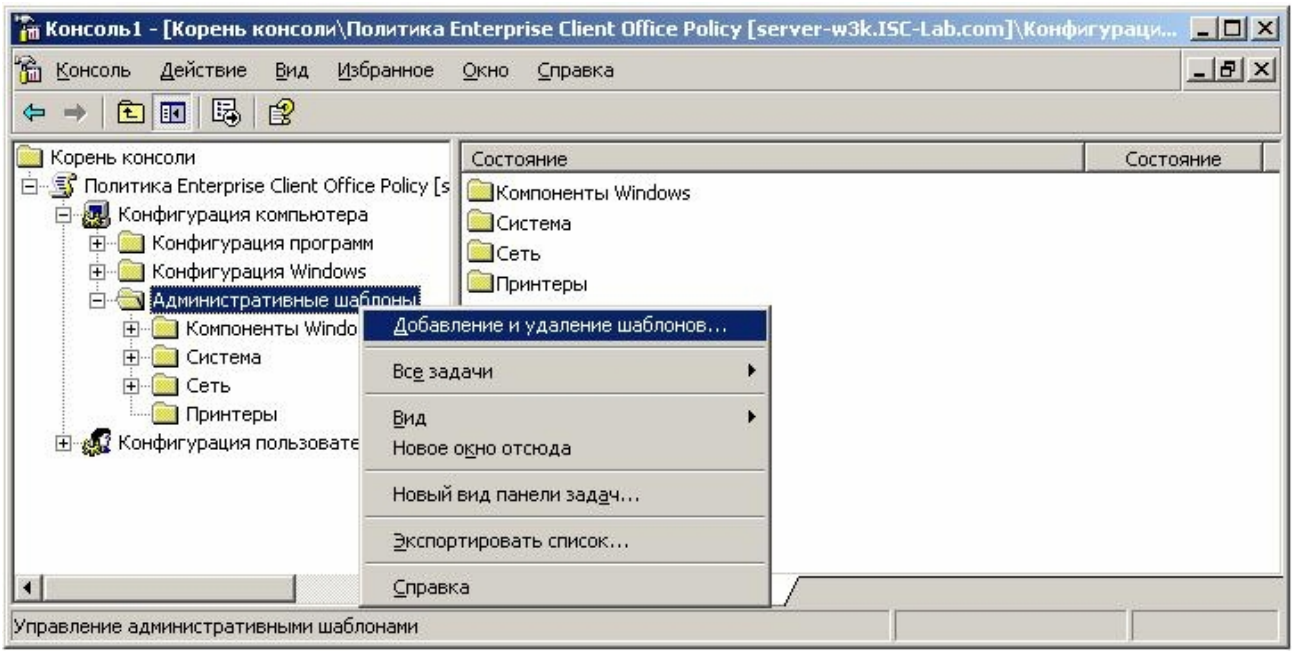


Рисунок 2.5

5. В появившемся диалоговом окне добавления и удаления шаблонов нажать кнопку «Добавить…». После чего в окне выбора шаблонов политики выделить административный шаблон `Office11.adm` и нажать «Открыть» (см. рисунок 2.6). При этом в дереве имен объектов оснастки консоли управления «Редактор объектов групповой политики» должна появиться папка «Microsoft Office 2003», содержащая настраиваемые для различных компонентов Microsoft® Office 2003 параметры безопасности (см. рисунок 2.7).

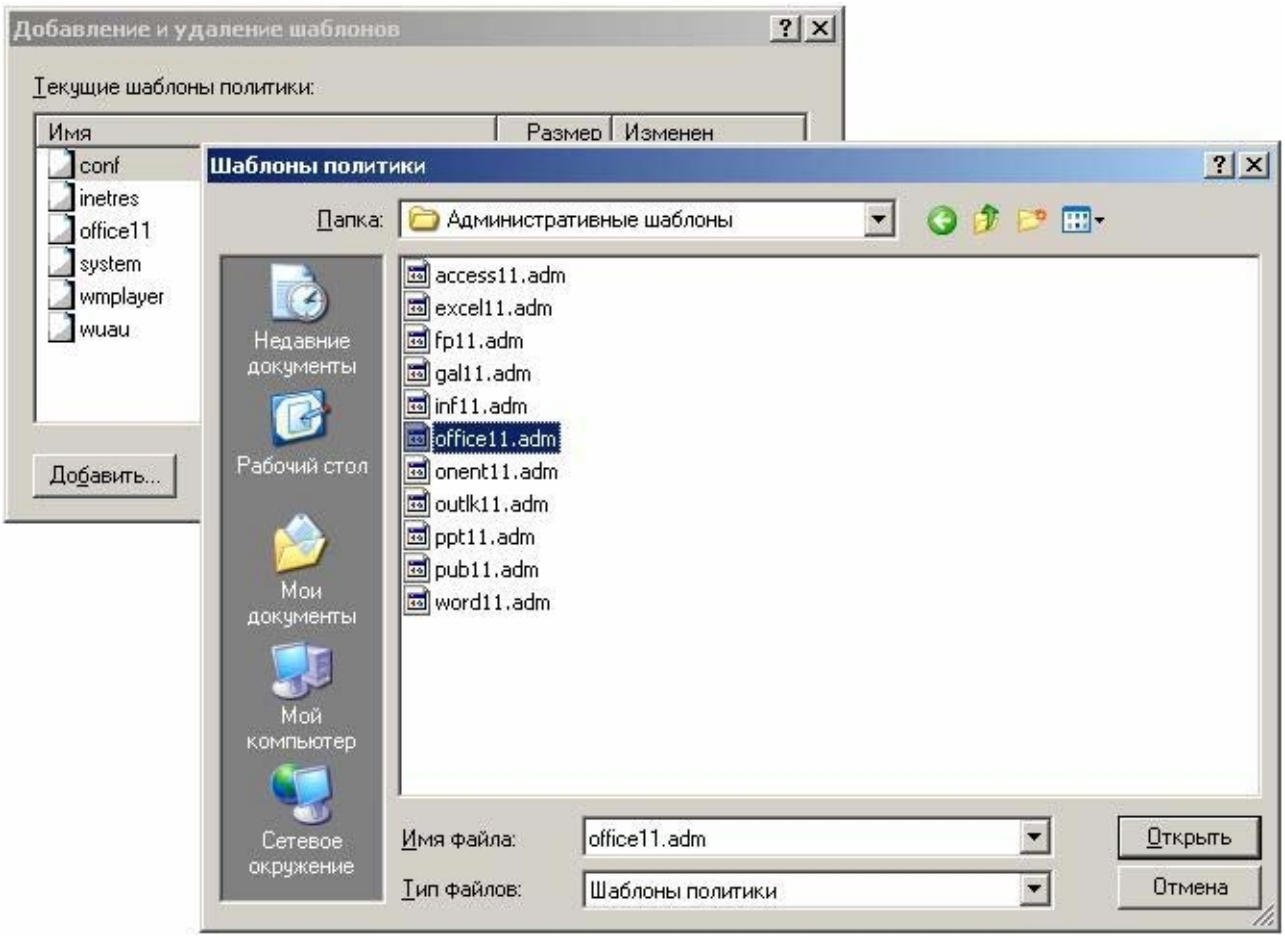


Рисунок 2.6

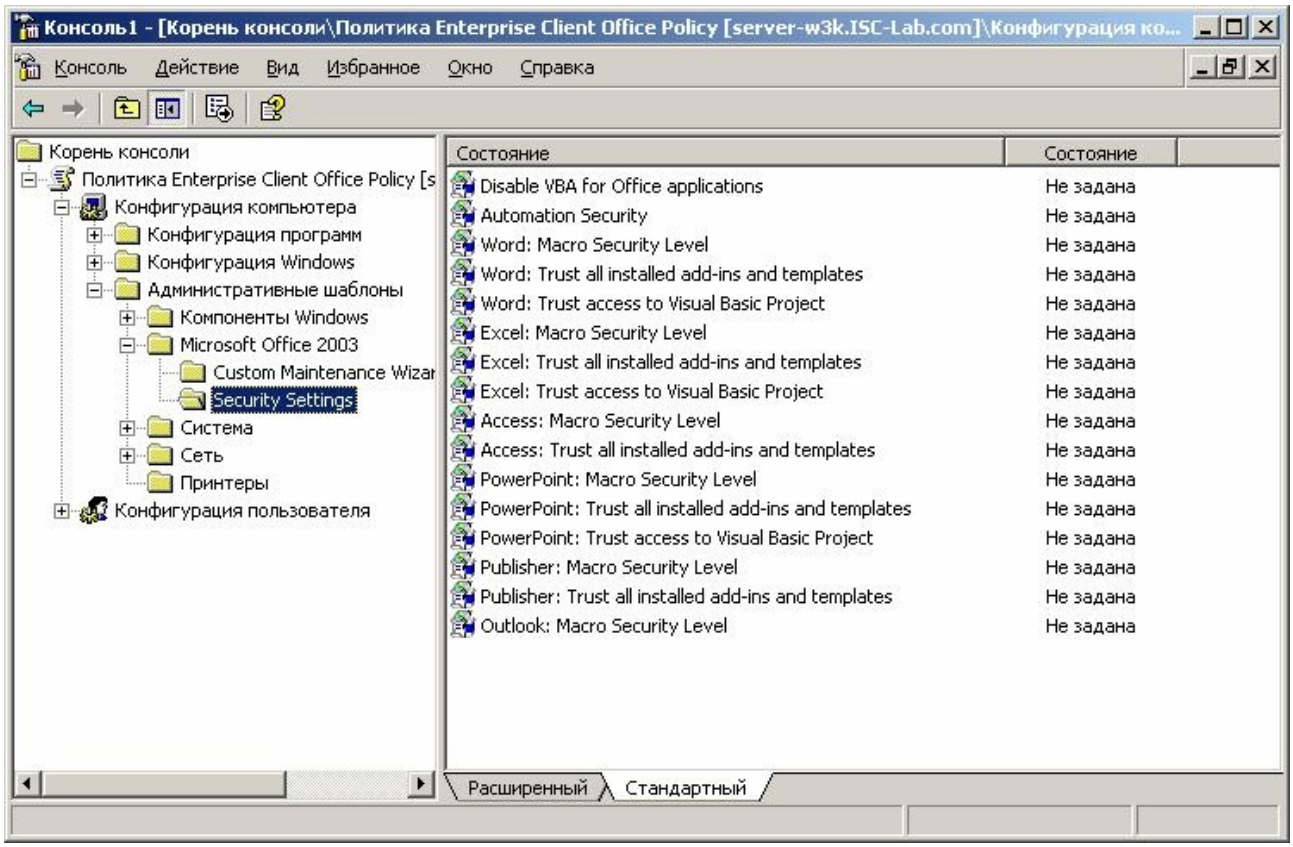


Рисунок 2.7

6. Выполнить настройку параметров безопасности офисного программного комплекса Microsoft® Office 2003. Для этого необходимо выполнить следующие действия:

- в дереве имен редактируемого объекта групповой политики последовательно развернуть узлы «Конфигурация компьютера», «Административные шаблоны», «Microsoft Office 2003» и «Security Settings». В результате в правой части окна редактора локального объекта групповой политики отобразятся параметры безопасности, настройку которых необходимо осуществить в соответствии с данными ниже рекомендациями;
- для настройки конкретного параметра безопасности открыть диалоговое окно его свойств;
- на вкладке «Параметр» выбрать требуемую опцию (например, «Включен») и рекомендуемое в соответствии с данным Руководством значение настраиваемого параметра безопасности Microsoft® Office 2003 (см. рисунок 2.8). Нажать «ОК»;

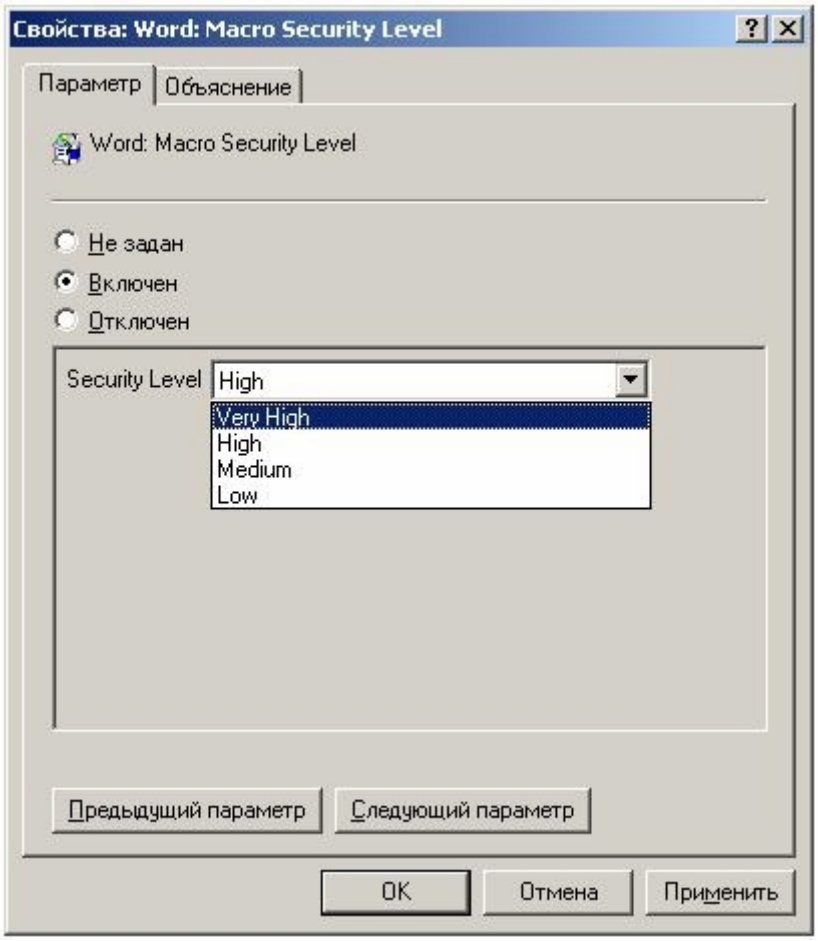


Рисунок 2.8

- выполнить выше описанные действия для всех настраиваемых параметров безопасности Microsoft® Office 2003;

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

Примечание: Рекомендуемые значения параметров в зависимости от конфигурации безопасности Microsoft® Office 2003 представлены в пп.2.4 настоящего Руководства.

При конфигурировании групповой политики на уровне организационного подразделения необходимо убедиться, что в списке управления доступом ACL объекта групповой политики для требуемой группы клиентских компьютеров определены разрешения «Чтение» и «Применение групповой политики». Если в списке управления доступом не будут определены требуемые значения разрешений, политика, определяющая параметры безопасности Microsoft® Office 2003, к указанным субъектам 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», что не позволит переопределить параметры безопасности, определяемые данной групповой политикой, другими объектами ОГП.

2.3 Порядок настройки Microsoft® Office 2003, установленного на автономном клиентском компьютере, в соответствии с конфигурациями «Enterprise» и «High Security»

2.3.1 Используемые административные шаблоны

С целью обеспечения требуемого уровня безопасности, необходимого для обработки конфиденциальной информации, на автономных компьютерах должна быть осуществлена настройка параметров безопасности офисного программного комплекса Microsoft® Office
2003 в соответствии с требуемой конфигурацией безопасности. Для приведения используемых в организации офисных программных комплексов Microsoft® Office 2003, установленных на клиентских компьютерах, к единой конфигурации безопасности необходимо выполнить настройку локальной политики безопасности на каждом компьютере. При этом для обеспечения отображения относящихся к Microsoft® Office 2003 параметров безопасности в дереве имен объектов оснастки консоли управления «Групповая политика» в окне редактора ОГП следует добавить административный шаблон `Office11.adm`.

2.3.2 Порядок добавления административного шаблона

Добавление административного шаблона `Office11.adm`, предоставляющего интерфейс настройки параметров безопасности различных компонентов, входящих в состав сертифицированной версии офисного программного комплекса Microsoft® Office 2003, необходимо осуществлять с использованием редактора локального объекта групповой политики. Чтобы добавить административный шаблон `Office11.adm` в локальный 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».

2. В окне консоли управления MMC (MMC – Microsoft Management Console) через пункт меню «Добавить или удалить оснастку» добавить оснастку «Групповая политика » и выбрать локальный объект групповой политики «Локальный компьютер» (см. рисунок 2.9 - 2.10).

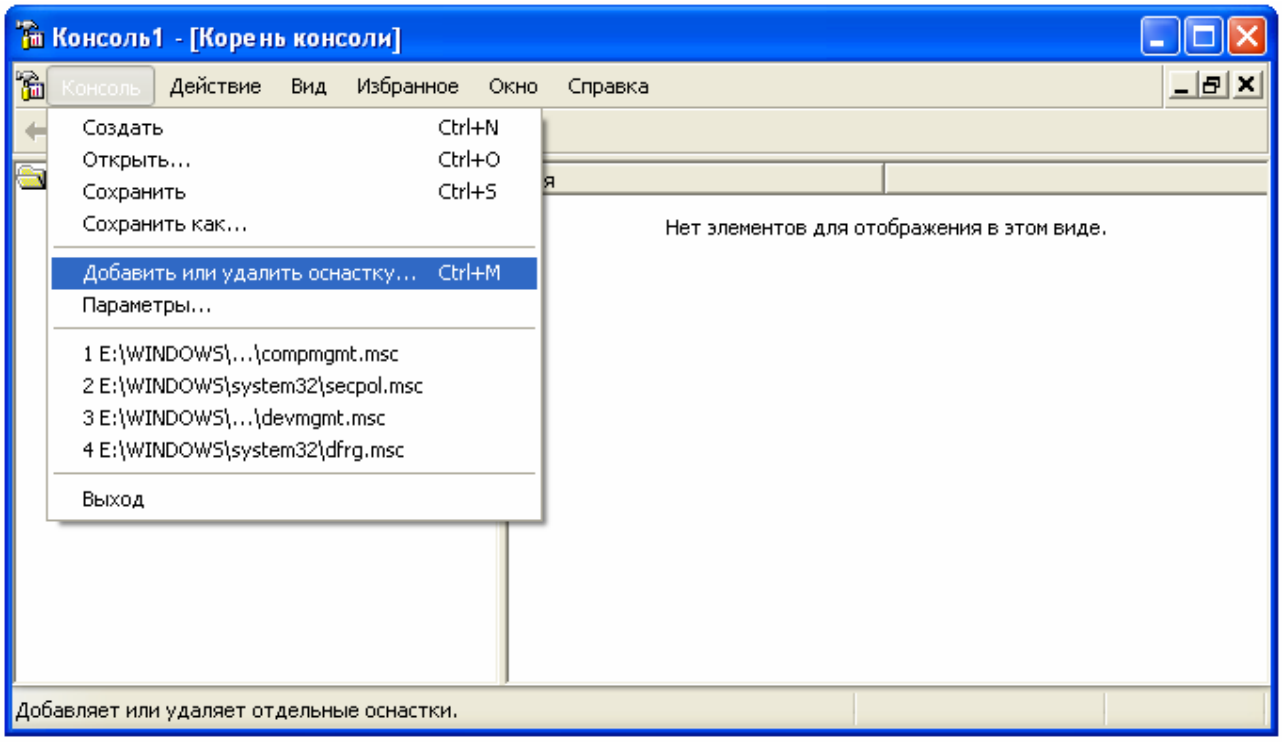


Рисунок 2.9

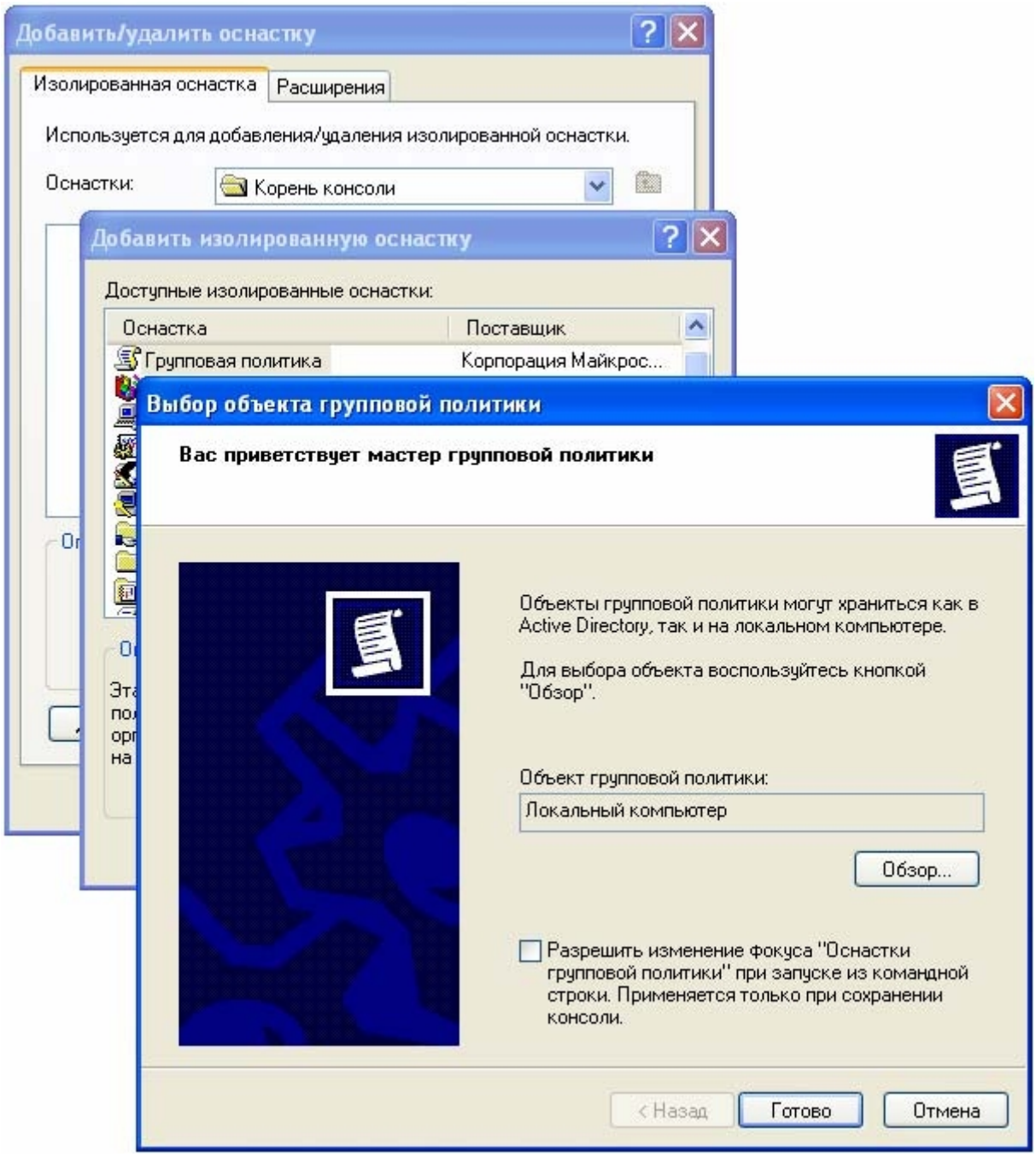


Рисунок 2.10

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

4. Правой кнопкой мыши нажать на элемент «Административные шаблоны» и в появившемся окне контекстного меню выбрать команду «Добавление и удаление шаблонов».

5. В появившемся диалоговом окне добавления и удаления шаблонов нажать кнопку «Добавить…». В открывшемся диалоговом окне выбора шаблонов политики выделить административный шаблон `Office11.adm` и нажать «Открыть» (см. рисунок 2.11). При этом в дереве имен объектов оснастки «Групповая политика» должна

появиться папка

«Microsoft Office 2003», содержащая настраиваемые для различных компонентов Microsoft® Office 2003 параметры безопасности (см. рисунок 2.12).

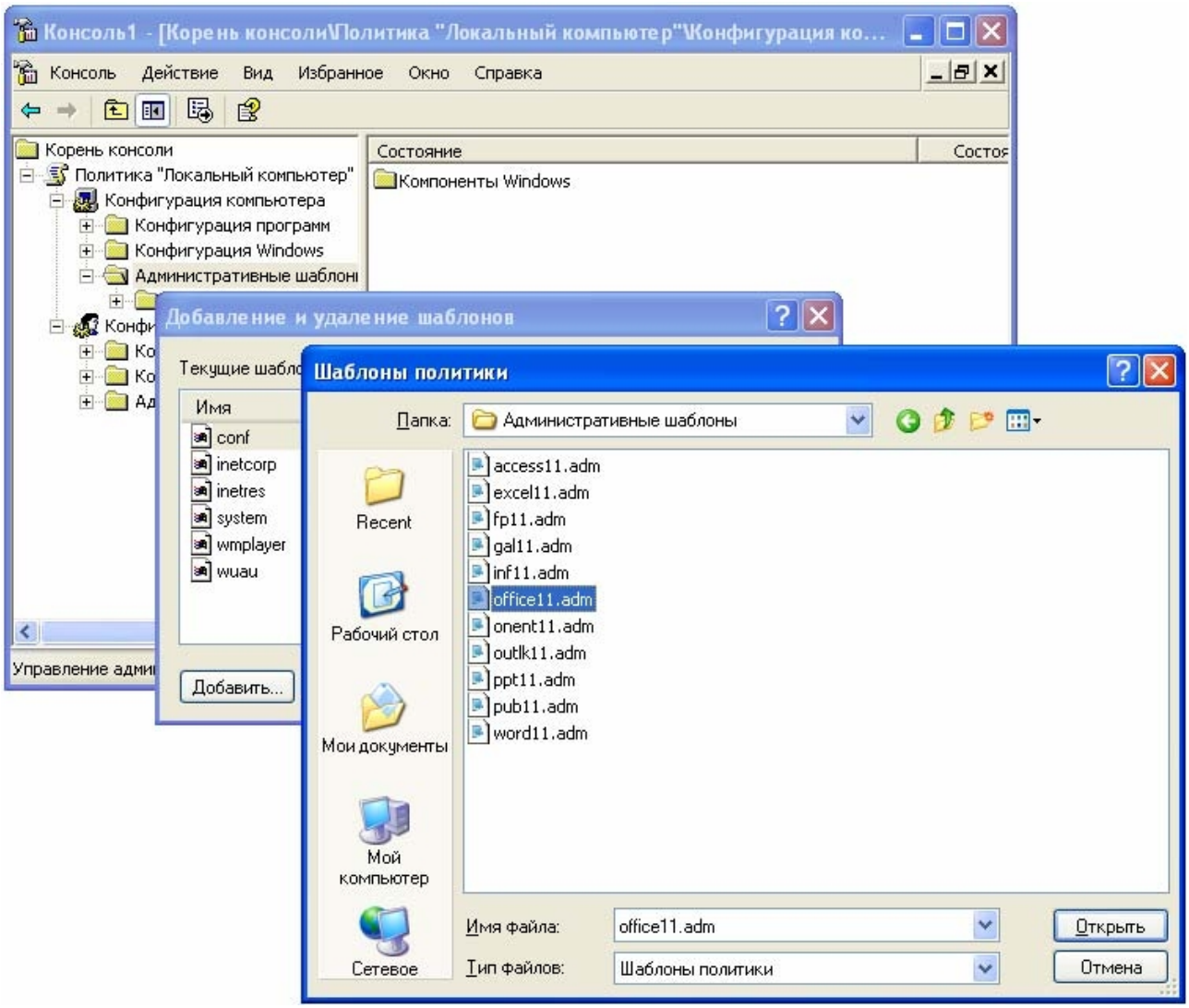


Рисунок 2.11

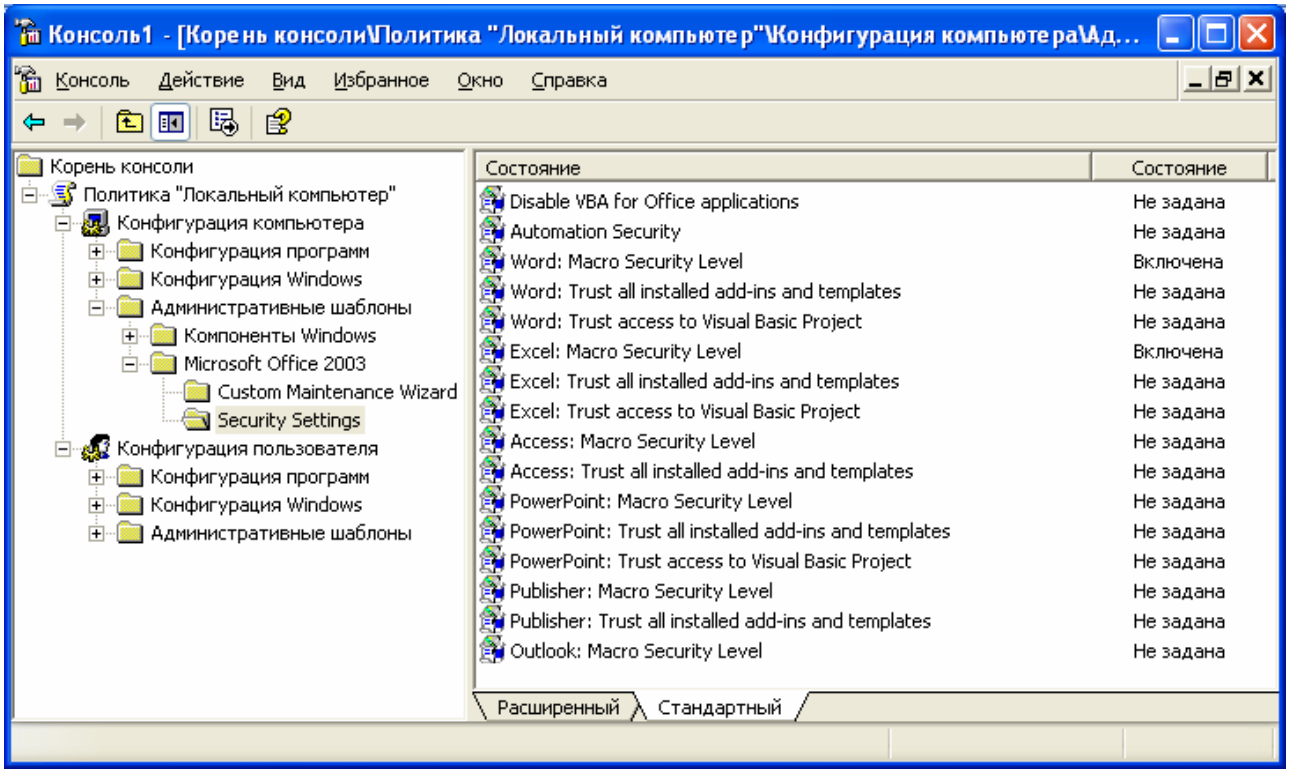


Рисунок 2.12

6. Выполнить настройку параметров безопасности офисного программного комплекса Microsoft® Office 2003. Для этого необходимо выполнить следующие действия:

- в дереве имен локального объекта групповой политики последовательно развернуть узлы «Конфигурация компьютера», «Административные шаблоны», «Microsoft Office 2003» и «Security Settings». В результате в правой части окна редактора локального объекта групповой политики отобразятся параметры безопасности, настройку которых необходимо осуществить в соответствии с данными ниже рекомендациями;
- для настройки конкретного параметра безопасности необходимо открыть диалоговое окно его свойств;
- на вкладке «Параметр» выбрать требуемую опцию (например, «Включен») и рекомендуемое значение настраиваемого параметра безопасности Microsoft® Office 2003 (см. рисунок 2.13). Нажать «ОК»;

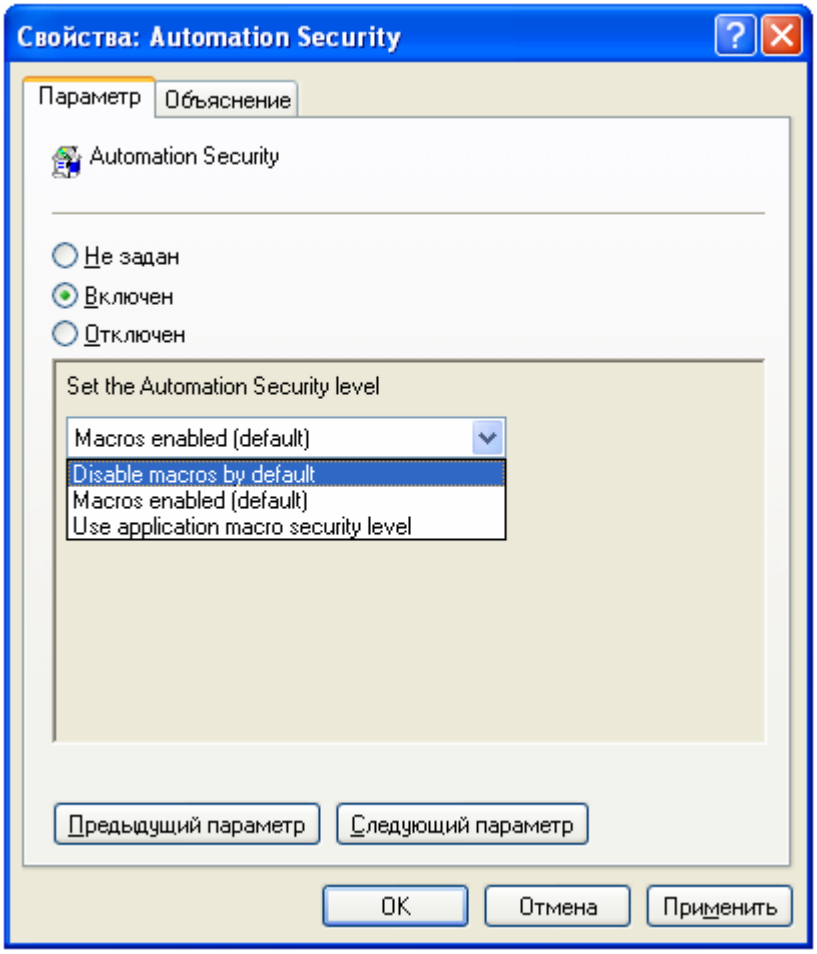


Рисунок 2.13

- выполнить указанные действия для всех настраиваемых параметров безопасности Microsoft® Office 2003;
- закрыть редактор объектов групповой политики;
- посредством команды `gpupdate /force` осуществить обновление параметров групповой политики.

Примечание: Рекомендуемые значения параметров в зависимости от конфигурации безопасности Microsoft® Office 2003 представлены в пп.2.4 настоящего Руководства.

2.4 Рекомендуемые параметры безопасности Microsoft® Office 2003 для конфигураций «Enterprise» и «High Security»

Параметры безопасности, представленные в данной главе, учитывают особенности конфигураций «Enterprise» и «High Security» и направлены, в первую очередь, на обеспечение защиты от макровирусов. В данном разделе рассматриваются основные параметры безопасности, для настройки которых используется групповая политика.

Применение рекомендованных параметров позволит обеспечить безопасную обработку информации с использованием офисного программного комплекса Microsoft® Office 2003.

Для обеспечения требуемого уровня безопасности с помощью редактора объектов групповой политики необходимо настроить параметры безопасности в следующем разделе пространства имен объекта групповой политики: Конфигурация компьютера\ Административные шаблоны \ Microsoft Office 2003\Security Settings.

Параметры **«Access: Trust all installed add-ins and templates»**

«Excel: Trust all installed add-ins and templates»

«PowerPoint: Trust all installed add-ins and templates»

«Publisher: Trust all installed add-ins and templates»

«Word: Trust all installed add-ins and templates»

Таблица 2.1 – Значение параметров

Конфигурации безопасности Microsoft® Office 2003	
«Enterprise Client»	**«High Security»**
Отключен	Отключен

Отключение параметров **«Trust all installed add-ins and templates»** (Доверять всем установленным надстройкам и шаблонам) для всех компонентов офисного программного комплекса Microsoft® Office 2003 позволит обеспечить возможность установки в приложениях Microsoft® Office 2003 только тех надстроек COM (надстройка - вспомогательная программа, служащая для добавления в Microsoft Office специальных команд или возможностей), которые имеют цифровую подпись и получены из надежных источников. При отключении данного параметра возможность установки неподписанных компонентов или компонентов, имеющих цифровую подпись ненадежных источников, определяется установленным для каждого приложения из состава Microsoft® Office 2003 уровнем безопасности для макросов:

- Very High (Очень Высокая): Разрешается запуск только макросов, установленных в надежных расположениях. Все остальные подписанные и неподписанные макросы отключаются;
- High (Высокая): Разрешается выполнение только макросов, имеющих цифровую подпись и полученных из надежных источников;

- `Medium` (Средняя): Решение о запуске потенциально опасных макросов принимается пользователем. При этом пользователь будет предупрежден о

потенциальном риске, связанном с использованием компонентов, не имеющих цифровой подписи, или макросов из источника, не входящего в список надежных;

- Low (Низкая): зашита от потенциально опасных макросов отсутствует. Надстройки и шаблоны могут загружаться и устанавливаться без участия пользователя.

Примечание: При настройке параметра «Trust all installed add–ins and templates» приложения Office рассматривают надстройки и шаблоны в качестве макросов.

Параметр **«Disable VBA for Office applications»**

Таблица 2.2 – Значение параметра

Конфигурации безопасности Microsoft® Office 2003	
«Enterprise Client»	**«High Security»**
Отключен	Включен

Параметр **«Disable VBA for Office applications»** (Запретить VBA для приложений Office) определят возможность использования в приложениях Microsoft® Office Excel 2003, Microsoft® Office Word 2003, Microsoft® Office PowerPoint 2003, Microsoft® Office Outlook 2003 и Microsoft® Office Publisher 2003 макроязыка программирования Visual Basic
для приложений (VBA - макро-версия языка программирования Microsoft Visual Basic, используемая для программирования приложений Microsoft Windows и поставляемая с некоторыми приложениями корпорации Microsoft).

Поддержка приложениями Office языка VBA зачастую трактуется как основная причина наличия брешей в системе безопасности Office и связанных с этим потенциальных угроз безопасности. Однако отключение в приложениях Office поддержки VBA не исключает полностью возможности запуска злонамеренного кода, поскольку, например, запуск элементов управления ActiveX может осуществляться и без VBA, но в тоже время предотвращает использование шаблонов, надстроек COM и макросов, которые потенциально могут содержать злонамеренный код. Таким образом, включение данного параметра делает использование приложений Office более безопасным, ограничивая вместе с тем возможность использования значительного числа функций Office. По этой причине включение параметра
«Disable VBA for Office applications» рекомендуется только в конфигурации «High Security».

Примечание: Отключение поддержки VBA может привести к тому, что пользователи

не смогут открыть некоторые файлы данных Office, содержащие макросы.

Параметры **«Excel: Macro Security Level »**

«PowerPoint: Macro Security Level »

«Publisher: Macro Security Level »

«Word: Macro Security Level »

«Outlook: Macro Security Level »

Таблица 2.3 – Значение параметра

Конфигурации безопасности Microsoft® Office 2003	
«Enterprise Client»	**«High Security»**
High (Высокая)	High (Высокая)

Макрос представляет собой последовательность команд и инструкций приложения, сгруппированных в виде отдельной команды с целью автоматизации выполнения соответствующей задачи. Макросы могут бытьполезны для автоматизации часто выполняемых задач. Хранение макросов может осуществляться как в документах, так и в шаблонах. В последнем случае макрос доступен в любом документе, созданном на основе шаблона.

Одна из важнейших задач приложений пакета Office связана с обеспечением безопасного использования макросов. Для ее решения в Microsoft® Office 2003 реализована поддержка четырех уровней безопасности для макросов, определяющих поведение системы

при загрузке и выполнении макросов, имеющих цифровую подпись и без наличия таковой. Подписывание макросов дает возможность разрешить выполнение лишь заранее указанных макросов. Имеется также возможность разрешить или запретить выполнение неподписанных макросов, а также составить список доверенных сертификатов, которые будут использоваться в организации для проверки подлинности.

Параметры **«Macro Security Level»** (Уровни безопасности для макросов) определяет следующие рекомендуемые уровни безопасности для макросов, устанавливаемые для конкретного приложения Office в рассматриваемых конфигурациях:

- `High (Высокая):` Разрешается выполнение только макросов, имеющих цифровую подпись и полученных из надежных источников. Выполнение неподписанных макросов автоматически запрещается, и файл открывается без каких-либо предупреждений.

В случае если администратором будет установлен уровень безопасности `Very High` (Очень высокая) при отключенном параметре «Доверять всем установленным надстройкам и

шаблонам», произойдет полное отключение всех макросов. При этом также будут отключены все надстройки COM и DLL-файлы смарт-тегов.

Примечание: Макросы, подписанные цифровым сертификатом, созданным самими пользователем, считаются недоверенными, поскольку такой сертификат выдан неофициальным центром сертификации. Поэтому они будут генерировать предупреждающие сообщения при установленном значении уровня безопасности для макросов «High» (Высокий).

Параметры **«Excel: Trust access to Visual Basic Project»**

«PowerPoint: Trust access to Visual Basic Project»

«Word: Trust access to Visual Basic Project»

Таблица 2.4 – Значение параметров

Конфигурации безопасности Microsoft® Office 2003	
«Enterprise Client»	**«High Security»**
Отключен	Отключен

Параметр **« Trust access to Visual Basic Project»** (Доверять доступ к Visual

Basic Project) определяет возможность доступа приложения к сопровождающему документ коду VBA. Отключение данного параметра позволяет обеспечить невозможность получения макросами, прикрепленными к открываемым пользователями файлам или документам, доступа к основным объектам, методам и свойствам Visual Basic. Исходя из этого, во всех рассматриваемых конфигурациях безопасности для указанных приложений Microsoft® Office

2003 данный параметр рекомендуется отключить.

Параметр **«Unsafe ActiveX Initialization»**

Таблица 2.5 – Значение параметра

Конфигурации безопасности Microsoft® Office 2003	
«Enterprise Client»	**«High Security»**
Prompt user to use control defaults	Prompt user to use control defaults

Параметр **«Unsafe ActiveX Initialization»** (Инициализация небезопасных элементов ActiveX) позволяет управлять инициализацией элементов управления Microsoft ActiveX (элемент управления ActiveX - элемент управления (такой как флажок

или кнопка), служащий для выбора параметров либо для запуска макроса или сценария,

автоматизирующего выполнение задачи) для всех установленных на компьютере приложений Microsoft® Office 2003.

Зачастую элементы управления ActiveX, содержащие злонамеренный код, используются для незаконного получения или уничтожения информации на клиентском компьютере. Для обеспечения требуемого уровня защиты при использовании управляющих элементов ActiveX в Microsoft® Office 2003 предусмотрены инструменты, которые позволяют определять возможность использования конечными пользователями только подписанных их создателями элементов ActiveX, обеспечивая, таким образом, определенную степень уверенности в их подлинности и безопасности.

В тоже время, включение параметра «Unsafe ActiveX Initialization» может вызвать определенные проблемы при просмотре документов или форм, содержащих элементы управления ActiveX. Поэтому перед включением данной опции рекомендуется протестировать все используемые в Microsoft® Office 2003 документы и формы.

Во всех рассматриваемых конфигурациях безопасности рекомендуется включить данный параметр, при этом его значение должно соответствовать «Prompt user to use control defaults» (Предлагать параметры по умолчанию). Данное значение позволит обеспечить загрузку безопасных для инициализации (SFI - Safe For Initialization) элементов управления ActiveX в безопасном режиме (safe mode) без запроса пользователя. В противном случае, при загрузке небезопасных для инициализации (UFI – Un-Safe For Initialization) элементов ActiveX, система проинформирует пользователя, что загружаемый элемент ActiveX является потенциально опасным и в случае отрицательного ответа, прекратит его загрузку. В случае согласия на инициализацию небезопасного элемента ActiveX, его загрузка будет осуществлена в соответствии с настройками, установленными по умолчанию.

2.5 Порядок копирования и контрольного суммирования пакета обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003

Для осуществления копирования пакета обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003 выполнить следующие действия:

1. Осуществить доступ к защищенному разделу сайта www.altx-soft.ru, содержащему перечень рекомендованных и обязательных к установке сертифицированных наборов исправлений безопасности и пакетов обновлений. Из имеющегося списка выбрать и осуществить копирование пакета обновления «Service

Pack 3». Для этого необходимо выполнить следующие действия:

- создать на локальном диске клиентского компьютера две директории, одна из которых в дальнейшем будет содержать копируемый с сайта пакет обновления «Service Pack 3», другая - утилиту контрольного суммирования «ФИКС-Light». При этом размер свободного дискового пространства должен быть достаточен для размещения данных суммарным объемом около 100 Мбайт;
- скопировать с защищенного сайта или с компакт-диска «Media Kit» на клиентский компьютер в созданную на предшествующем шаге директорию утилиту контрольного суммирования «ФИКС-Light»;
- скопировать на клиентский компьютер в соответствующую директорию пакет обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003. Для этого на защищенном сайте необходимо осуществить выбор опции «выбрать», которая сопоставлена со ссылкой на пакет обновления

  «Service Pack 3», размещенный на сайте корпорации Microsoft. В результате данного действия будет выполнено перенаправление запроса на копирование пакета обновления на соответствующий раздел сайта корпорации Microsoft. Далее, следуя представленным на сайте корпорации Microsoft указаниям, осуществить копирование пакета обновления «Service Pack 3» непосредственно с сайта корпорации Microsoft в ранее созданную директорию на локальном диске клиентского компьютера. По окончанию процесса копирования в указанной директории должен появиться файл с именем `OFFICE2003SP3-KB923618-FULLFILE-RUS.EXE`, содержащий файлы пакета обновления «Service Pack 3»;
- провести контрольное суммирование скопированного пакета обновления «Service Pack 3» с использованием утилиты контрольного суммирования «ФИКС-Light». Для этого в режиме командной строки осуществить вызов утилиты контрольного суммирования «ФИКС-Light» (`FixLight.exe`) со следующими параметрами:

  `FixLight.exe <File1> [<File2>]`, где

  `<File1>` - параметр, определяющий полный путь к имени суммируемого файла (в случае с пакетом обновления «Service Pack 3» имя суммируемого файла соответствует значению `OFFICE2003SP3-KB923618-FULLFILE-RUS.EXE`);

  `<File2>` - необязательный параметр, определяющий полный путь к имени

файла результатов контрольного суммирования пакета обновления (по умолчанию, соответствует значению `.\Result\_Rez.txt`). При этом результаты контрольного суммирования пакета обновления могут быть

помещены в директорию, дочернюю по отношению к директории, содержащей утилиту «ФИКС-Light», либо в любую иную директорию, указанную пользователем.

Например, для контрольного суммирования пакета обновления «Service Pack 3», скопированного в директорию `c:\ServicePack3`, и размещении результатов контрольного суммирования (файл `Fix_SP3.txt`) в директории `c:\Result_SP2` необходимо выполнить команду:

```
FixLight.exe c:\ServicePack3\OFFICE2003SP3-KB923618-FULLFILE-RUS.EXE c:\Result_SP3\Fix_SP3.txt
```

В случае если второй параметр не указан, будет использовано значение по умолчанию, т.е. файл результатов контрольного суммирования пакета обновления «Service Pack 3» с именем `_Rez.txt` будет размещен в директории `Result`, дочерней по отношению к директории, содержащей утилиту «ФИКС-Light».

2. По окончанию контрольного суммирования пакета обновления «Service Pack 3» вернуться на защищенный сайт и выбрать опцию «Отправить отчет», сопоставленную со ссылкой на данный пакет обновления, после чего в появившемся диалоговом окне указать путь к директории на локальном диске клиентского компьютера, содержащей файл результатов контрольного суммирования скопированного пакета обновления «Service Pack 3». В результате на защищенном сайте будет выполнено сравнение результатов контрольного суммирования скопированного пакета обновления с эталонной контрольной суммой пакета обновления «Service Pack 3», размещенной на защищенном сайте и связанной
с указанным обновлением.

2.6 Порядок установки пакета обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003

Для установки пакета обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003 необходимо выполнить следующие действия:

1. Перед началом установки пакета обновления «Service Pack 3» осуществить резервное копирование операционной системы (для чего воспользоваться утилитой `ntbackup.exe` или специализированными средствами резервного копирования/ восстановления данных сторонних производителей) и выполнить завершение работы всех программ.

2. Инициировать процесс установки пакета обновления «Service Pack 3», при этом установка может осуществлять как с использованием графического интерфейса Windows при участии пользователя, так и в автоматическом режиме с использованием командной строки.

Примечание: Перед установкой пакета обновления «Service Pack 3» убедитесь, что служба «Windows Installer» запущена. В противном случае установка будет невозможна.

Порядок установки пакета обновления «Service Pack 3» в режиме командной строки

Для автоматической установки пакета обновления «Service Pack 3» необходимо выполнить следующие действия:

1. Извлечь содержимое пакета обновления «Service Pack 3» в заданную папку на локальном диске клиентского компьютера. Для этого необходимо осуществить вызов окна командной строки и выполнить следующую команду:

`OFFICE2003SP3-KB923618-FULLFILE-RUS.EXE/Q /C /T:c:\SP3_Update`,

где `OFFICE2003SP3-KB923618-FULLFILE-RUS.EXE`– имя файласкопированного пакета обновления «Service Pack 3»;

`/Q` – параметр, исключающий вывод диалогового окна состояния во время извлечения содержимого пакета обновления;

`/C` - параметр, исключающий вывод предложения указать имя папки, в которую будут помещены извлекаемые файлы;

`/T` – параметр, указывающий полный путь к директории, в которую будут извлекаться файлы. В качестве примера указана папка `c:\SP3_Update`.

2. Осуществить редактирование файла `ohotfix.ini`, описывающего параметры конфигурации установщика пакета обновления «Microsoft Office Hotfix Installer». В частности, установить следующие значения для параметров конфигурации, изменив поведение по умолчанию:

- `ShowSuccessDialog = 0` – параметр, определяющий режим установки пакета обновления без вывода финального диалогового окна, уведомляющего об его успешной установке;
- `OHotfixUILevel = q` – параметр, исключающий вывод диалоговых окон, информирующих пользователя о ходе установки пакета обновления;
- `MsiUILevel = q` – параметр, исключающий вывод диалоговых окон, формируемых установщиком Windows Installer;

- `RebootInQuietMode = 0` – параметр, определяющий необходимость принудительной перезагрузки операционной системы после установки пакета обновления, в случае если в этом возникнет необходимость.

Примечание: Чтобы установщик «Microsoft Office Hotfix Installer» следовал установленным параметрам конфигурации, необходимо, чтобы файл ohotfix.ini был расположен в том же самом каталоге, что и сам установщик (ohotfix.exe).

3. Инициировать процесс установки пакета обновления «Service Pack 3», осуществив посредством двойного нажатия кнопкой мыши запуск исполняемого файла `ohotfix.exe` установщика пакета обновления «Microsoft Office Hotfix Installer», расположенного в папке, содержащей извлеченные файлы пакета обновления.

4. Проанализировать содержимое системного журнала «Приложение» на предмет окончания обновления офисного программного комплекса Microsoft® Office 2003 и возможных ошибок, которые могли при этом возникнуть.

При соблюдении указанных выше рекомендаций установка пакета обновления «Service Pack 3» для офисного программного пакета Microsoft® Office 2003 будет осуществлена в автоматизированном скрытом режиме, не требующем какого-либо вмешательства со стороны пользователей.

Порядок установки пакета обновления «Service Pack 2» с использование графического интерфейса Windows

Администратор имеет возможность установить пакет обновления «Service Pack 3» в диалоговом режиме, выполнив следующие действия:

1. Инициировать процесс установки пакета обновления «Service Pack 3», осуществив посредством двойного нажатия кнопкой мыши запуск исполняемого файла `OFFICE2003SP3-KB923618-FULLFILE-RUS.EXE`, содержащего дистрибутив пакета обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003.

2. После извлечения файлов (см. рисунок 2.14) дождаться окончания установки пакета обновления «Service Pack 3».

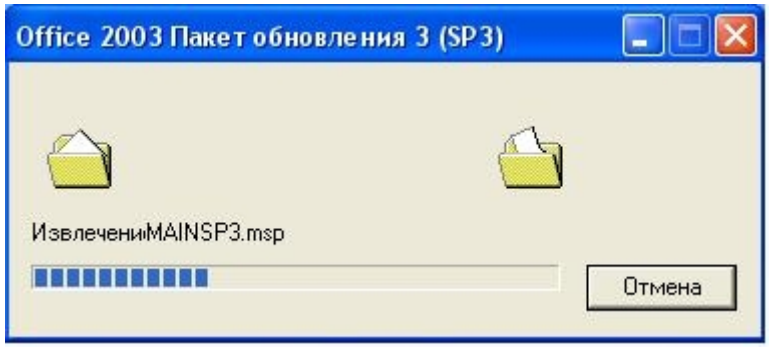


Рисунок 2.14

3. По окончанию установки пакета обновления «Service Pack 3» проанализировать содержимое журналов регистрации на предмет возможных ошибок, которые могли возникнуть в процессе установки.

4. Выполнить идентификацию и проверку корректности установки пакета обновления «Service Pack 3» для офисного программного комплекса Microsoft® Office 2003:

- посредством оснастки «Сведения о системе» определить текущую версию установленных компонентов офисного программного комплекса Microsoft® Office 2003 (см. рисунок 2.15). Таблица соответствия версий исполняемых файлов Microsoft® Office 2003 представлена ниже;

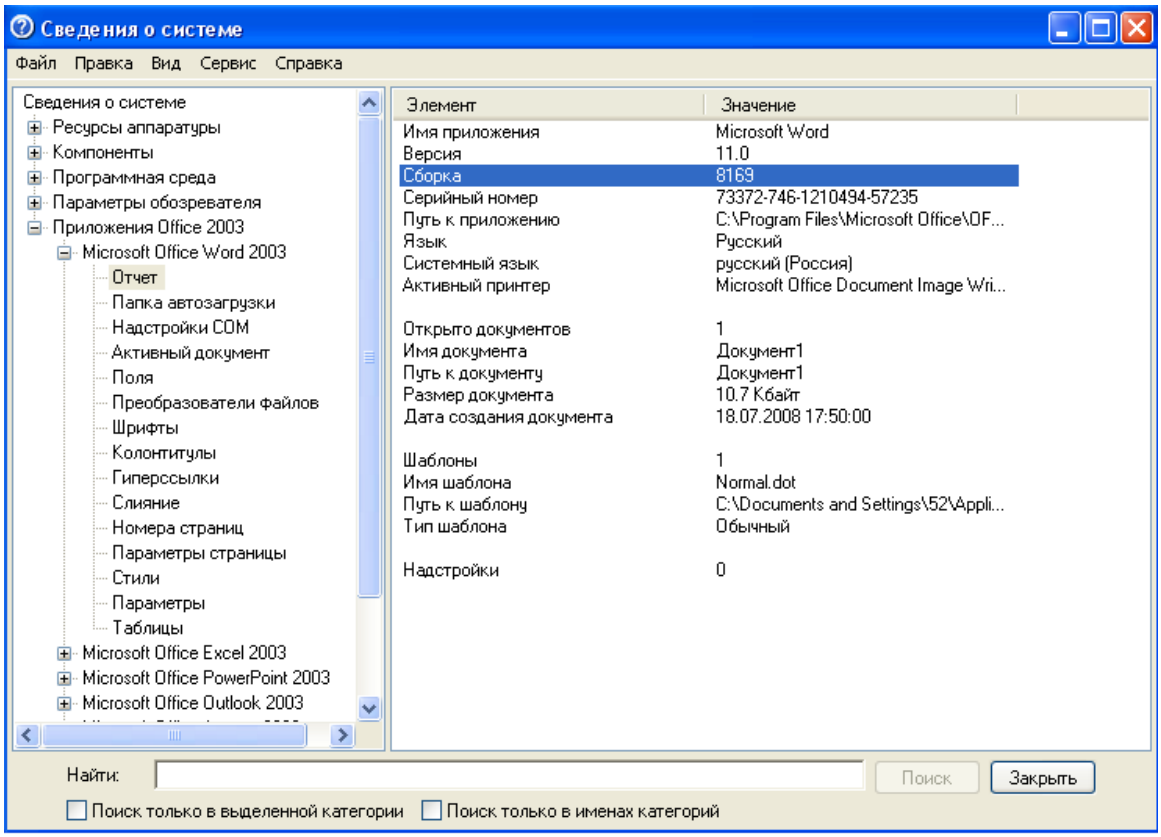


Рисунок 2.15

Таблица 2.6

№ п/п	Компонент Microsoft® Office 2003	Имя исполняемого файла	Версия исполняемого файла
1.	Microsoft® Office Exel 2003	Excel.exe	11.0.8169.0
2.	Microsoft® Office Access 2003	Msaccess.exe	11.0.8166.0
3.	Microsoft® Office Publisher 2003	Mspub.exe	11.0.8166.0
4.	Microsoft® Office Outlook® 2003	Outlook.exe	11.0.8169.0
5.	Microsoft® Office PowerPoint® 2003	Powerpnt.exe	11.0.8169.0
6.	Microsoft® Office Word 2003	Winword.exe	11.0.8169.0

- в окне «Установка и удаление программ» панели управления в списке установленных программ идентифицировать версию офисного программного комплекса Microsoft® Office 2003 (см. рисунок 2.16);

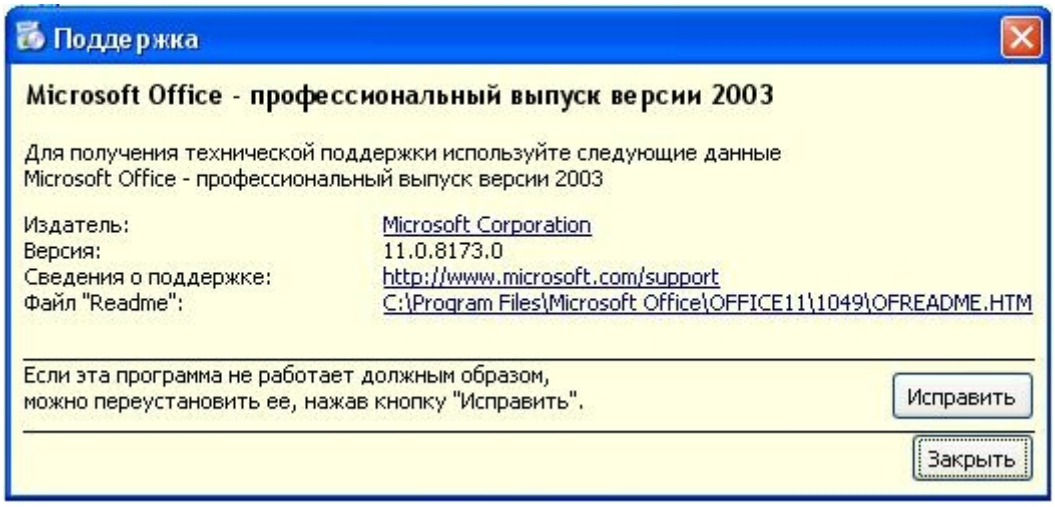


Рисунок 2.16

- проконтролировать следующие изменения, произошедшие в реестре:
  - в подразделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\11.0\Common\ProductVersion` значение строкового параметра `LastProduct`, отражающего текущую версию офисного программного комплекса Microsoft® Office 2003, должно соответствовать «`11.0.8173.0`» (см. рисунок 2.17);

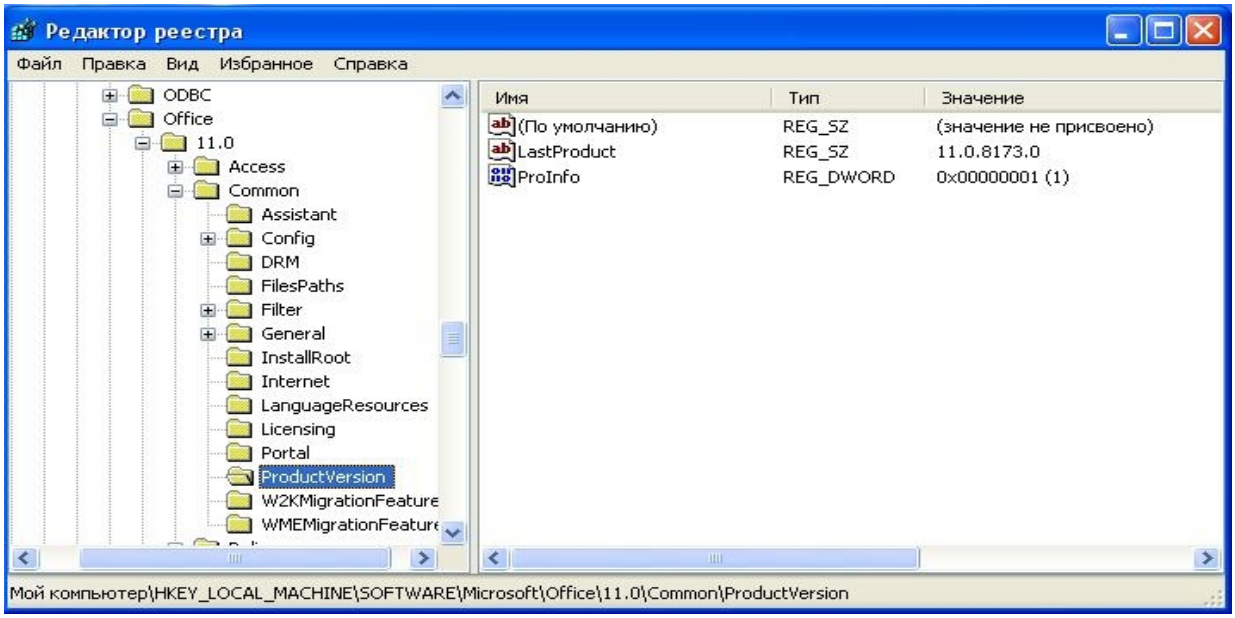


Рисунок 2.17

2.7 Порядок копирования и установки наборов исправлений безопасности для офисного программного комплекса Microsoft® Office 2003

Для осуществления установки набора (наборов) исправлений безопасности для офисного программного комплекса Microsoft® Office 2003 необходимо осуществить доступ к защищенному разделу сайта www.altx-soft.ru, содержащему перечень рекомендованных и обязательных к установке сертифицированных наборов исправлений безопасности или пакетов обновлений, выбрать из имеющегося списка требуемый набор исправлений безопасности, осуществить его копирование и контрольное суммирование в соответствии с последовательностью действий, рассмотренной в пп.2.5 настоящего Руководства.

По окончанию контрольного суммирования набора исправлений безопасности вернуться на защищенный раздел сайта и выбрать опцию «Отправить отчет», сопоставленную со ссылкой на данный набор исправлений, после чего в появившемся диалоговом окне указать путь к директории на локальном диске клиентского компьютера, содержащей файл результатов контрольного суммирования скопированного набора исправлений безопасности. В результате на защищенном сайте будет выполнено сравнение результатов контрольного суммирования скопированного набора исправлений безопасности с эталонной контрольной суммой набора исправлений безопасности, размещенной на защищенном сайте и связанной с указанным обновлением.

Для установки набора исправлений безопасности для офисного программного

комплекса Microsoft® Office 2003 необходимо выполнить следующие действия:

1. Перед началом установки набора исправлений безопасности завершить работу всех программ, входящих в состав офисного программного комплекса Microsoft® Office 2003.
2. Осуществить резервное копирование операционной системы (для чего воспользоваться утилитой `ntbackup.exe` или специализированными средствами резервного копирования/ восстановления данных сторонних производителей).
3. Инициировать процесс установки набора исправлений безопасности, при этом установка может быть осуществлена как с использованием графического интерфейса Windows при участии пользователя, так и в автоматическом режиме с использованием интерфейса командной строки.
4. Проанализировать журналы регистрации событий операционной системы с целью обнаружения возможных ошибок, возникших на этапе установки набора исправлений безопасности.

3 Последовательность действий по контролю сертифицированной версии Microsoft® Office 2003

3.1 Контроль маркирования сертифицированной версии офисного программного комплекса Microsoft® Office 2003

Контроль маркирования сертифицированной версии офисного программного комплекса «Microsoft® Office, Профессиональный выпуск 2003, Русская версия» в совокупности с контролем исходного состояния, основанном на контрольном суммировании, направлен на получение удостоверения в том, что на клиентском компьютере установлена сертифицированная версия офисного программного комплекса Microsoft® Office 2003.

Контроль маркирования проводится следующим образом:

1. Удостовериться, что на упаковочной коробке дистрибутива офисного программного комплекса, установленного на компьютере, присутствует надпись «Microsoft® Office, Профессиональный выпуск 2003, Русская версия».

2. Удостовериться, что упаковочная коробка дистрибутива офисного программного комплекса, установленного на компьютере, маркирована знаком соответствия сертифицированной продукции.

3. Удостовериться, что на оптическом носителе дистрибутива офисного программного комплекса, установленного на компьютере, присутствует надпись «Microsoft® Office, Профессиональный выпуск 2003, Русская версия».

3.2 Автоматизированный контроль сертифицированной версии офисного программного комплекса Microsoft® Office 2003

Для контроля версии и настроек безопасности офисного программного комплекса Microsoft® Office 2003 может использоваться «Программа контроля сертифицированной версии офисного программного комплекса Microsoft® Office 2003 Service Pack 3 (SP3)», поставляемая дополнительно к дистрибутиву на компакт-диске. Установка программы осуществляется путем копирования каталога, содержащего дистрибутив программы, на жесткий магнитный диск компьютера.

Запуск программы на исполнение осуществляется путем выбора исполняемого файла OfficeChk.exe и двойного щелчка левой кнопкой мыши на его пиктограмме и должен выполняться пользователем, обладающим

административными полномочиями в операционной системе. После запуска программы контроля сертифицированной версии

офисного программного комплекса Microsoft® Office 2003 на экране должно появиться диалоговое окно, представленное на рисунке 3.1.

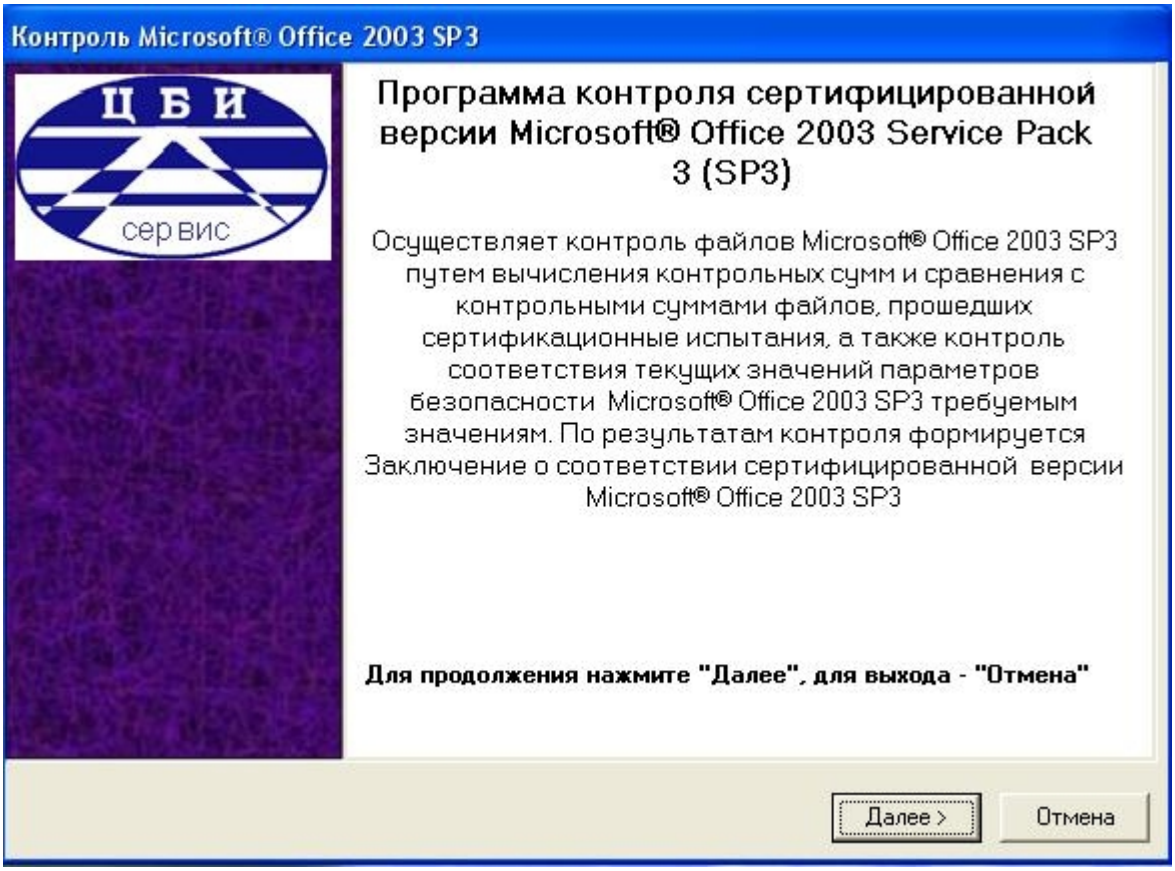


Рисунок 3.1 – Вид окна программы контроля сертифицированной версии Microsoft® Office 2003

При запуске программа выполняет контроль версии и редакции установленного на компьютере офисного программного комплекса Microsoft® Office. В случае если версия или редакции Microsoft® Office не соответствует сертифицированной, в диалоговом окне программы будет выдано соответствующее предупреждение и дальнейшие действия по проверке будут невозможны (см. рисунок 3.2).

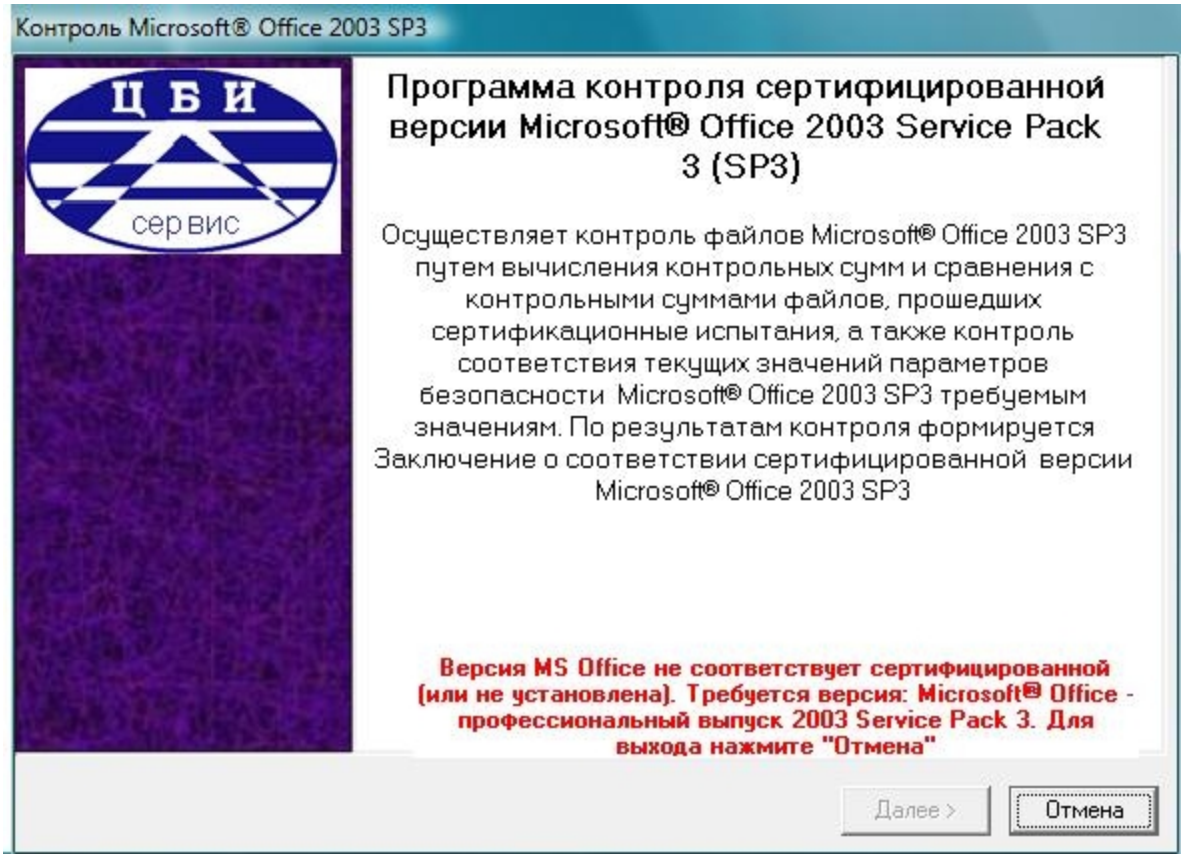


Рисунок 3.2 – Вид окна программы в случае несоответствия версии и редакции установленного Microsoft® Office

В случае если соответствие версии и редакции установлено, после нажатия кнопки «Далее» инициируется процесс контроля соответствия контрольных сумм исполняемых файлов и текущих настроек безопасности офисного программного комплекса Microsoft® Office 2003, установленного на компьютере, эталонным сертифицированным значениям. После успешного завершения контроля соответствия контрольных сумм файлов и настроек безопасности окно программы примет вид, представленный на рисунке 3.3.

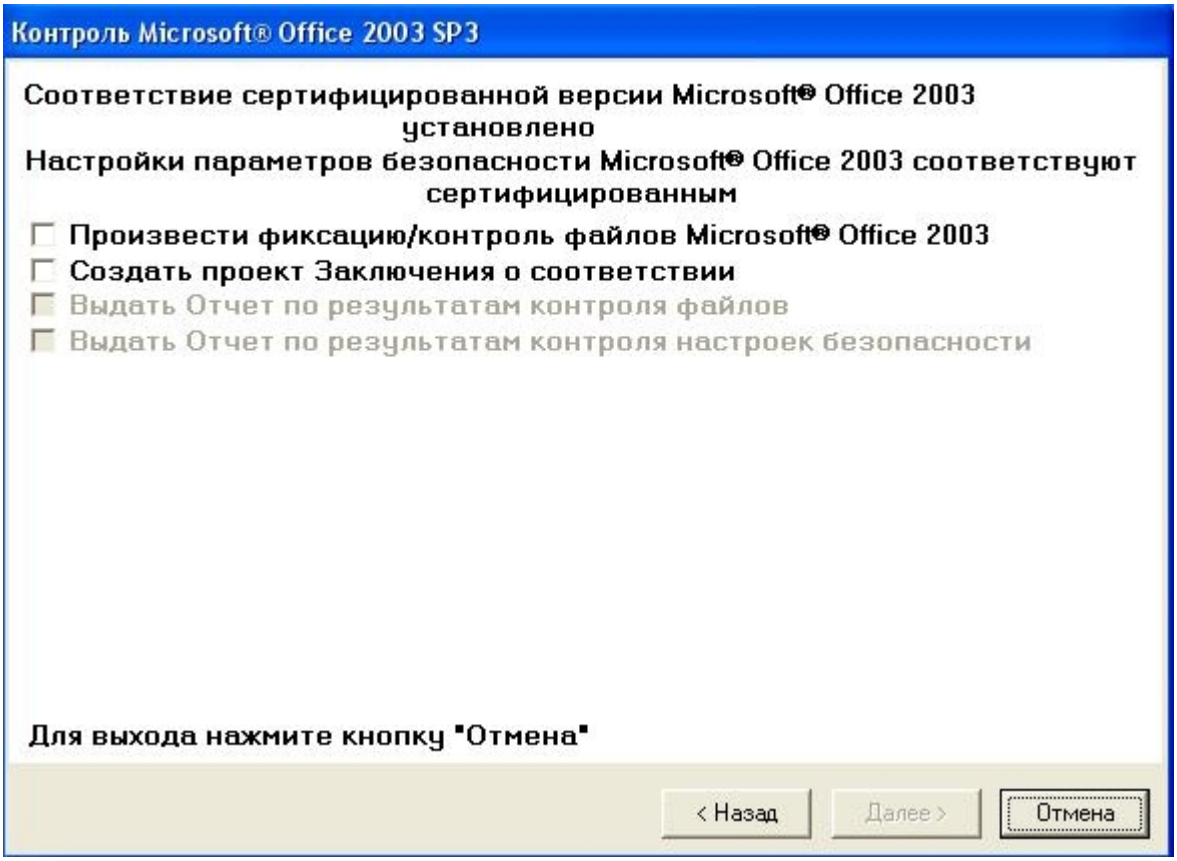


Рисунок 3.3 – Вид окна программы контроля сертифицированной версии Microsoft® Office 2003 после успешного завершения контроля

При установлении соответствия контрольных сумм файлов сертифицированной версии Microsoft® Office 2003, но несоответствии настроек безопасности (например, уровня защиты от макросов для Microsoft® Word) окно программы контроля будет иметь вид, представленный на рисунке 3.4.

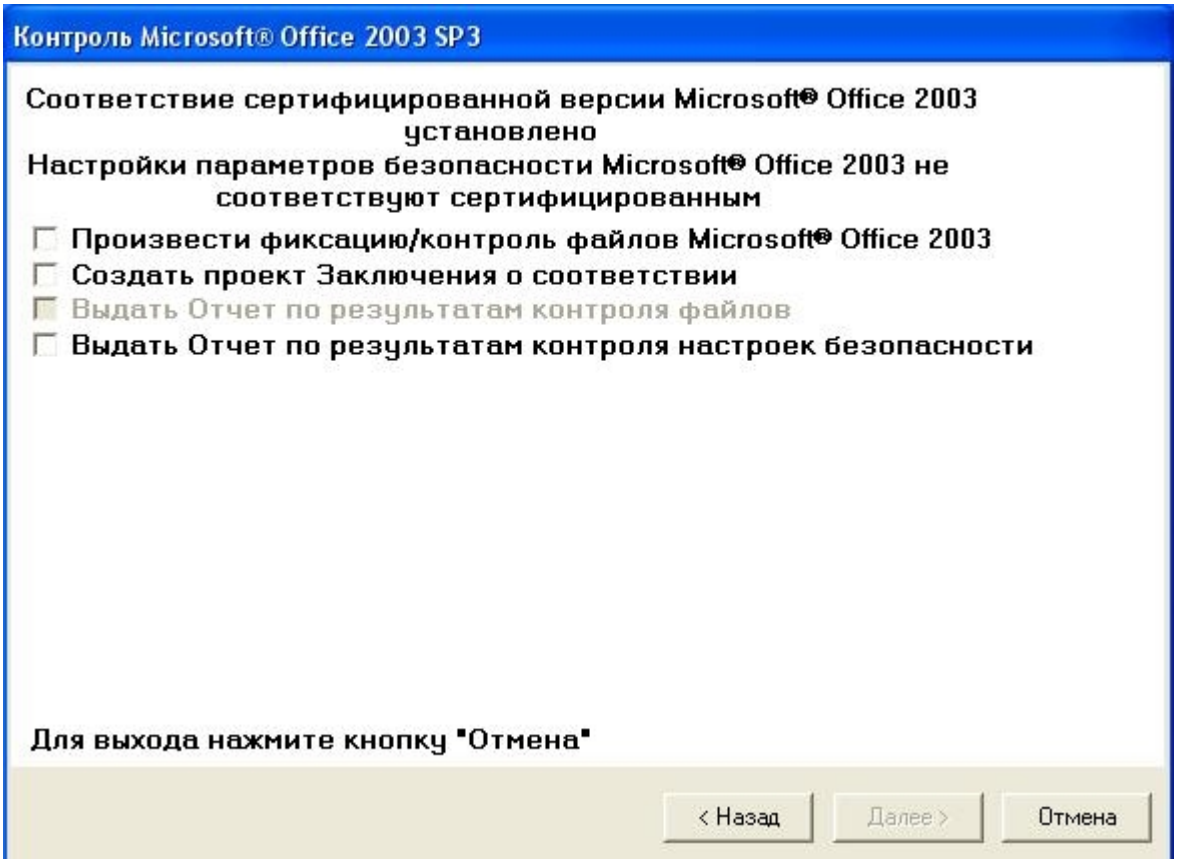


Рисунок 3.4 – Вид окна программы контроля сертифицированной версии Microsoft® Office 2003 при несоответствии настроек безопасности

Если соответствие контрольных сумм исполняемых файлов офисного программного комплекса, инсталлированного на компьютере, не установлено (по причине отсутствия указанных файлов) либо установлено частично, окно программы контроля сертифицированной версии Microsoft® Office 2003 примет следующий вид (см. рисунок 3.5).

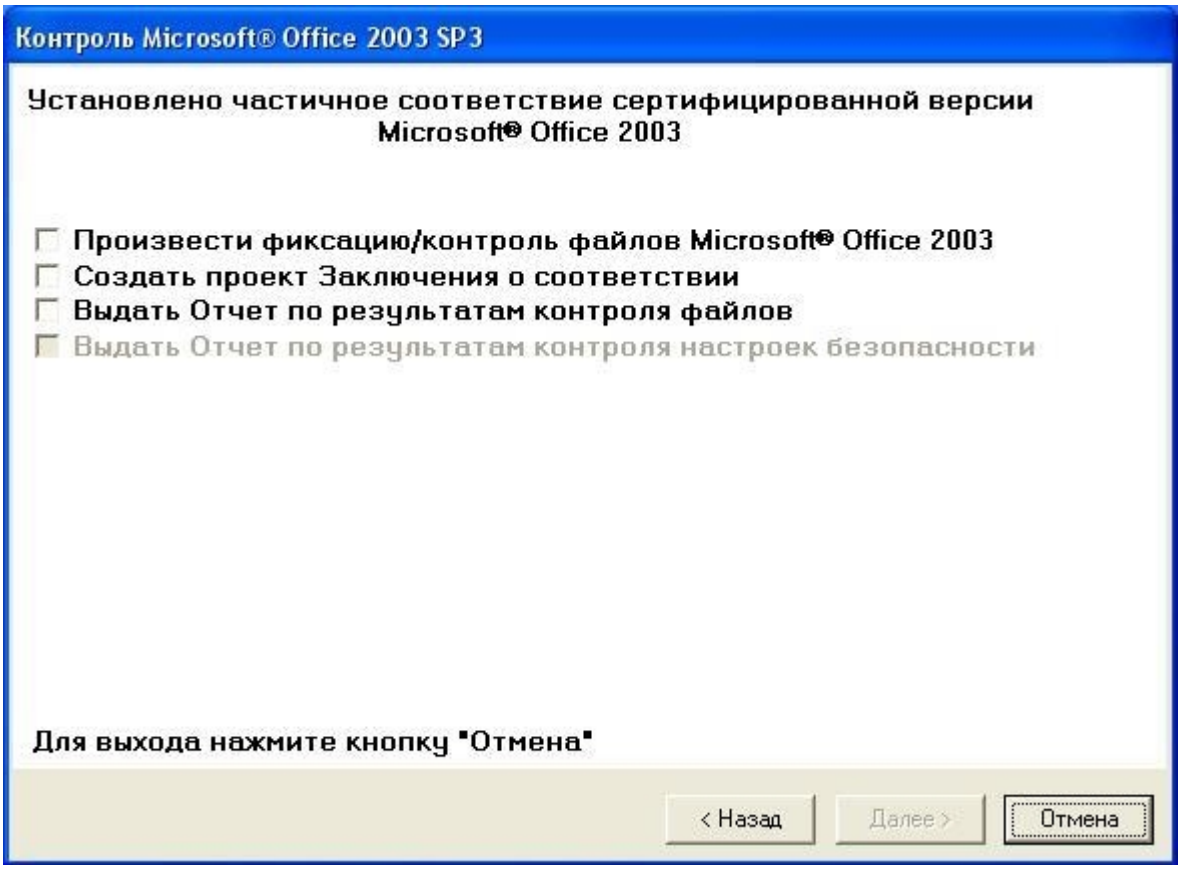


Рисунок 3.5 – Вид окна программы контроля сертифицированной версии Microsoft® Office 2003 при несоответствии контрольных сумм

Если на компьютере инсталлированы только некоторые компоненты из состава офисного программного комплекса «Microsoft® Office, Профессиональный выпуск 2003» (например, Microsoft® Word и Microsoft® Outlook), соответствие контрольных сумм исполняемых файлов для которых было установлено, окно программы контроля сертифицированной версии Microsoft® Office 2003 примет следующий вид (см. рисунок 3.6).

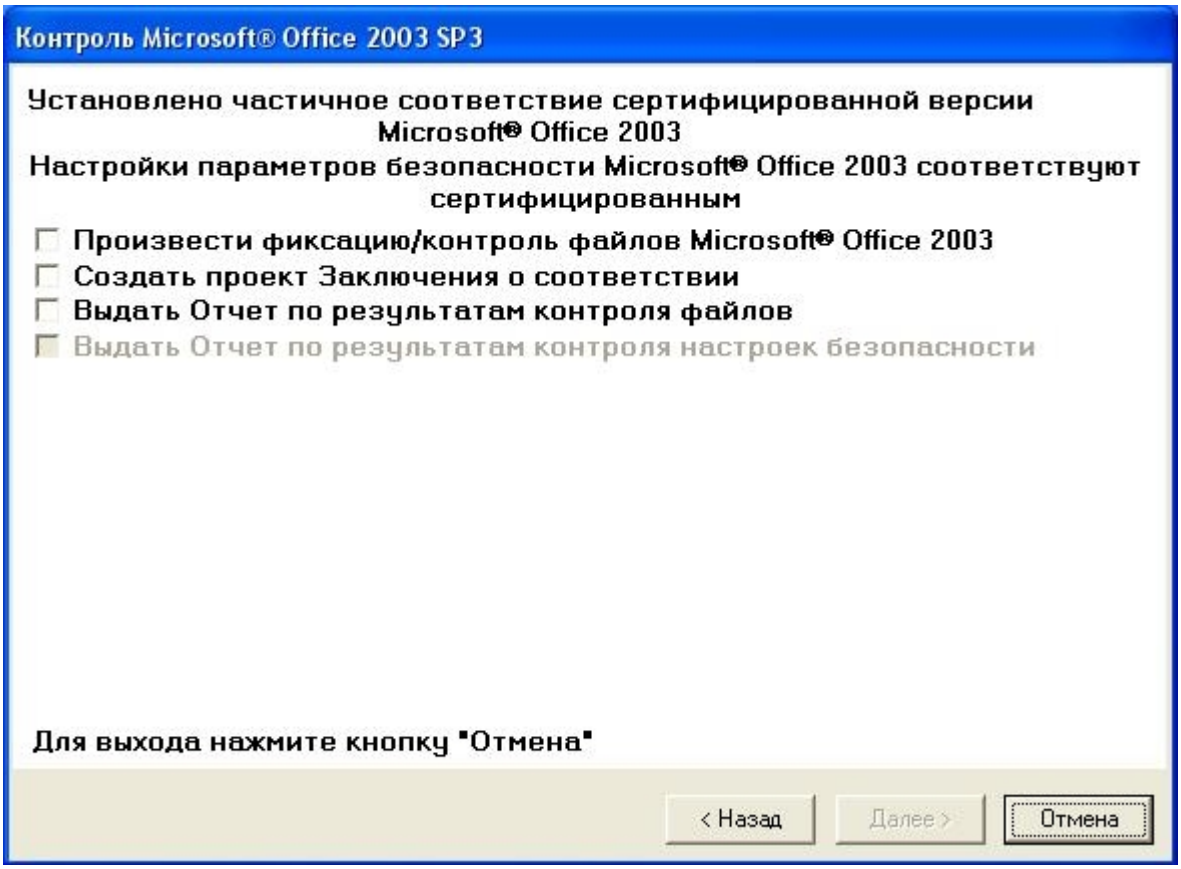
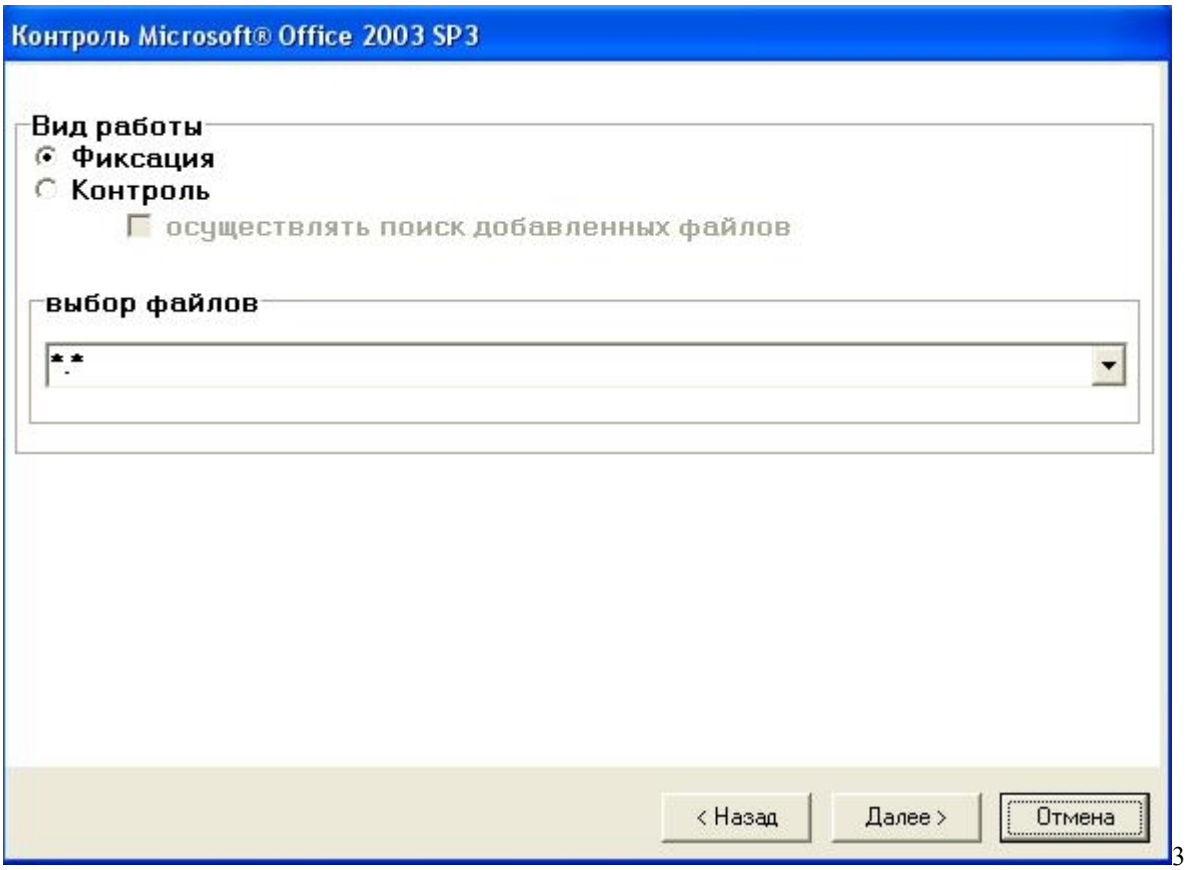


Рисунок 3.6 – Вид окна программы контроля сертифицированной версии при выборочной установке Microsoft® Office 2003

Для создания отчета по результатам контроля настроек безопасности офисного программного комплекса Microsoft® Office 2003 необходимо выбрать опцию «Выдать Отчет по результатам контроля настроек безопасности» и нажать кнопку «Далее». Анализ результатов контроля позволит выявить и в дальнейшем устранить существующие несоответствия между текущими и требуемыми настройками безопасности.

Для получения заключения о результатах контроля офисного программного комплекса Microsoft® Office 2003 необходимо выбрать опцию «Выдать проект Заключения о соответствии» и нажать кнопку «Далее».

Для проведения фиксации исходного состояния файлов Microsoft® Office 2003 необходимо выбрать опцию «Произвести фиксацию/контроль исходного состояния файлов Microsoft® Office 2003» и в появившемся диалоговом окне программы, представленном на рисунке 3.7, установить переключатель «Вид работы» в положение «Фиксация».



3

Рисунок 3.7 – Вид окна программы при проведении фиксации или контроля исходного состояния файлов Microsoft® Office 2003

По умолчанию в поле «Выбор файлов» указана маска, предполагающая проведение фиксации всех файлов Microsoft® Office 2003, 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 «Далее», окно программы приобретет вид, показанный на рисунке 3.8.

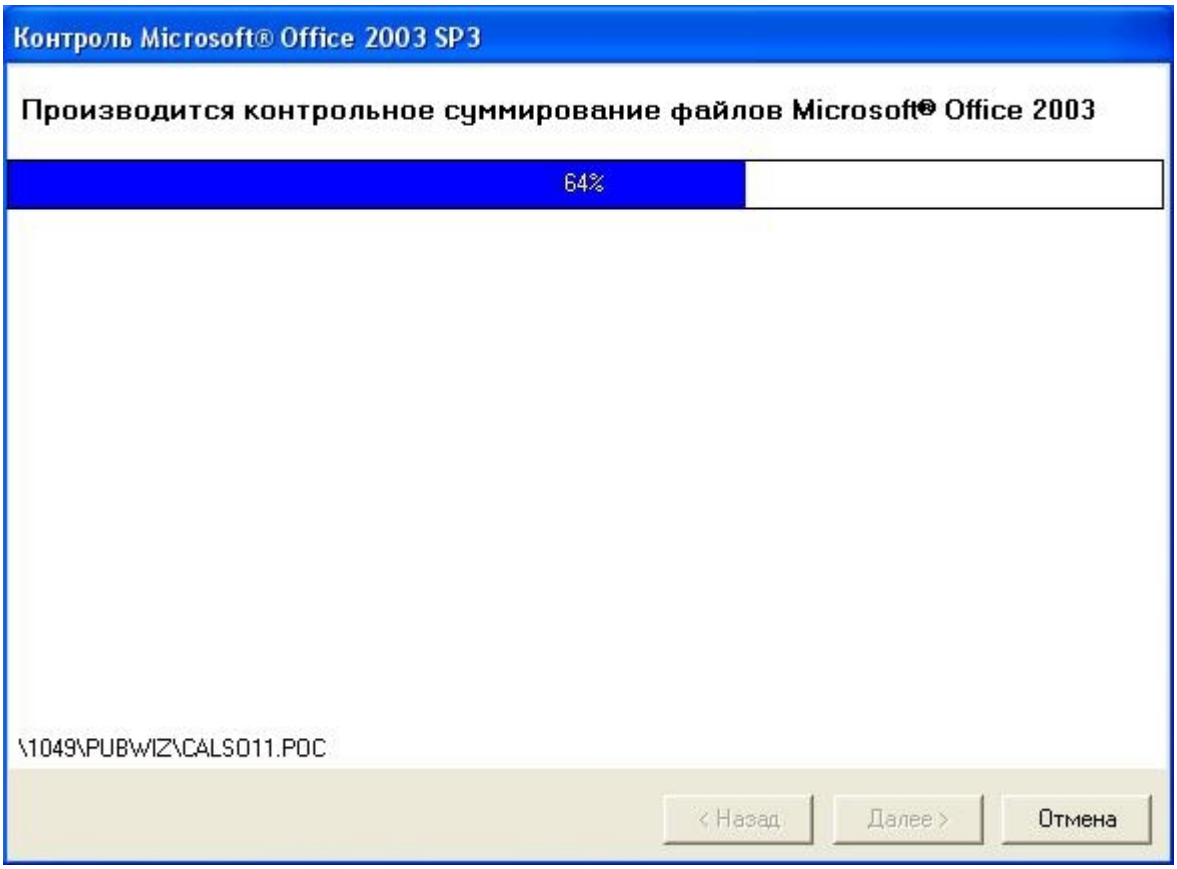


Рисунок 3.8 – Вид окна программы при проведении контрольного суммирования файлов Microsoft® Office 2003

После завершения контрольного суммирования в появившемся диалоговом окне необходимо ввести имя файла, в который необходимо сохранить результаты фиксации исходного состояния файлов Microsoft® Office 2003 для последующего контроля.

Для проведения контроля исходного состояния необходимо установить переключатель «Вид работы» в положение «Контроль». Для обнаружения в процессе контроля файлов, добавленных в папку, необходимо выбрать опцию «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 «Далее» 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 3.9.

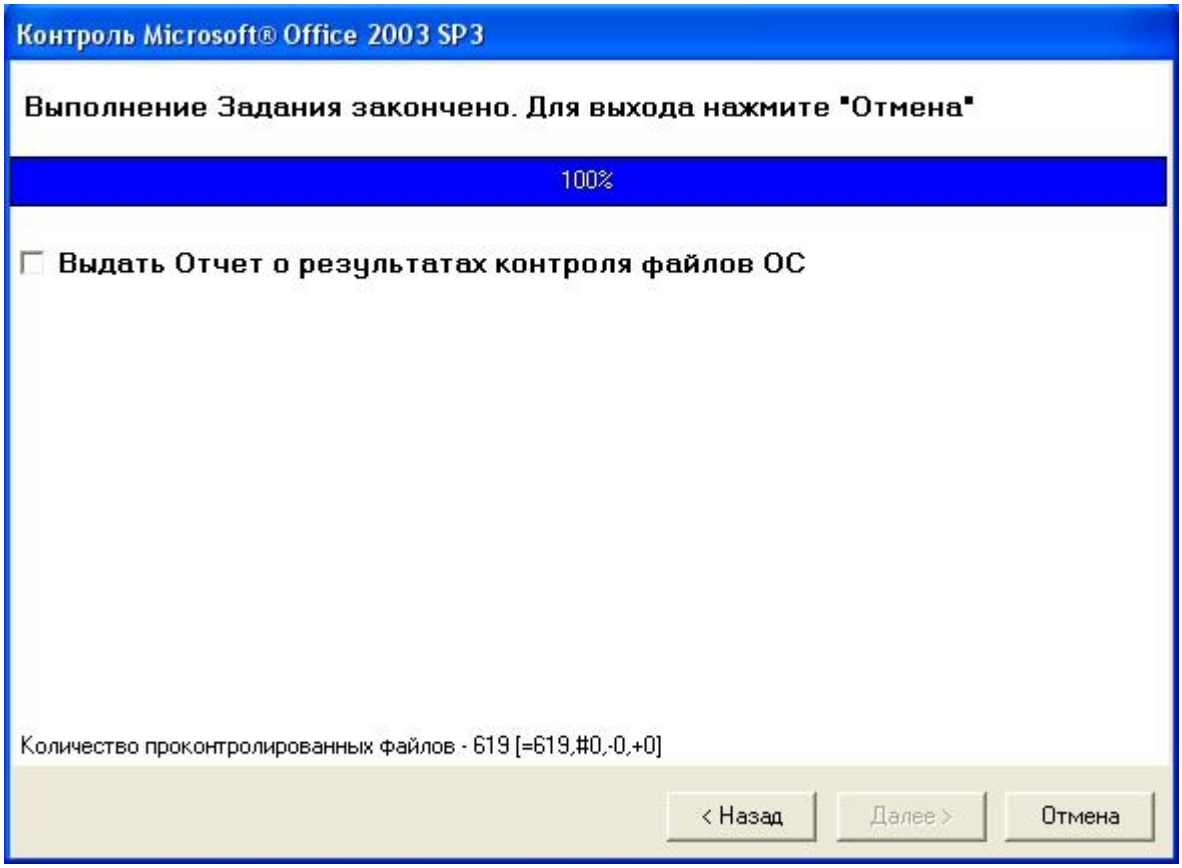


Рисунок 3.9 – Вид окна программы при проведении контроля исходного состояния файлов Microsoft® Office 2003

В нижней части окна представлен обобщенный результат контроля – количество проконтролированных файлов. В скобках рядом указаны три или четыре цифры. Рядом со знаком «=» расположено число файлов, не изменившихся после выполнения фиксации. Рядом со знаком «#» - количество измененных файлов, рядом со знаком «-» - количество отсутствующих файлов, рядом со знаком «+» - число файлов, добавленных в папку с программными файлами Microsoft® Office 2003 (только при установленной опции «Осуществлять поиск добавленных файлов»).

Проведение контроля целостности рекомендуется осуществлять при появлении подозрений на вирусы, нарушении исправного функционирования Microsoft® Office 2003, после установки программного обеспечения и т.п.