ЦЕНТР БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Операционная система
WINDOWS® VISTA™ Service Pack 1

Руководство по безопасной настройке и контролю сертифицированной версии

2008

Оглавление

1Область применения

Настоящий документ (далее – Руководство) представляет собой руководство по организации защиты конфиденциальной информации на объекте информатизации с установленной сертифицированной версией операционной системы WINDOWS® VISTA™ Service Pack 1 .

Руководство предназначено для сотрудников эксплуатирующих организаций, ответственных за защиту информации, и позволяет настроить операционную систему WINDOWS® VISTA™ Service Pack 1 в соответствии с той конфигурацией, в которой данное изделие было сертифицировано.

Руководство также содержит описание комплекса организационных мероприятий по защите информации на объекте информатизации в соответствии с документом «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К).

Руководство разработано с учетом результатов сертификационных испытаний операционной системы WINDOWS® VISTA™ Service Pack 1 по требованиям безопасности информации и согласованно с Гостехкомиссией России и компанией Microsoft.

2 Настройка сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1

2.1 Конфигурации сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1

Операционная система WINDOWS® VISTA™ Service Pack 1 сертифицирована для использования в конфигурациях «Enterprise Client» и «High Security».

Конфигурация «Enterprise Client»

Данная конфигурация подразумевает наличие инфраструктуры домена Active Directory Windows Server 2003 R2 или Windows Server 2003 с пакетом обновления (SP1, SP2). Управление клиентскими компьютерами в данной среде происходит через использование групповой политики, применяемой на различных уровнях иерархии (сайты, домены, организационные подразделения). Групповые политики предоставляют механизм централизованного управления политиками безопасности для среды функционирования в целом.

Конфигурация «High Security»

Конфигурация High Security подразумевает наличие более ограничивающей политики безопасности и усиленные настройки безопасности для клиентов. При применении данных настроек функциональность пользователя ограничивается полномочиями на выполнение только необходимых задач. Полномочия пользователя определяются политикой ограниченного использования программ и разрешенными службами.

2.2 Настройка операционной системы WINDOWS® VISTA™ Service Pack 1 в конфигурациях Enterprise Client и High Security

2.2.1 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:

- контейнеры групповой политики Group Policy Container (GPC), расположенные в Active Directory;
- шаблоны групповой политики Group Policy Template (GPT), размещенные в файловой системе.

Шаблоны безопасности

Под шаблоном безопасности понимается физическое представление конфигурации безопасности, т.е. шаблон безопасности представляет собой текстовый файл, в котором определены параметры безопасности операционной системы. Каждый шаблон храниться в обычном текстовом файле с расширением *.inf*, что позволяет копировать, импортировать и экспортировать параметры безопасности.

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

Для изменения шаблонов используется редактор (оснастка) шаблонов безопасности из состава оснасток консоли управления Microsoft Management Console (MMC) или текстовый редактор (например, программа «Блокнот»). Шаблоны безопасности содержат все параметры

безопасности, назначаемые объекту групповой политики, кроме относящихся к политикам открытых ключей и политике IPSec. Некоторые разделы шаблона могут содержать списки управления доступом Access Control List (ACL), которые определенны на языке Security Descriptor Definition Language (SDDL).

В таблице 2.1 показано соответствие между разделами групповой политики и секциями файла шаблона безопасности.

Таблица 2.1 – Формат шаблона безопасности

Раздел групповой политики	Раздел шаблона безопасности
Account Policy	[System Access]
Audit Policy	[System Log] [Security Log] [Application Log]
User Rights	[Privilege Rights]
Security Options	[Registry Values]
Event Log	[Event Audit]
Restricted Groups	[Group Membership]
System Services	[Service General Setting]
Registry	[Registry Keys]
File System	[File Security]

Шаблоны безопасности, позволяющие настроить систему в соответствии с той конфигурацией, в которой данное изделие было сертифицировано

.

2.2.2Параметры безопасности клиентских компьютеров под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Параметры безопасности, представленные в данной главе, учитывают особенности конфигураций «Enterprise Client» и «High Security». В данном разделе рассматриваются основные параметры безопасности, для настройки которых в домене используется групповая политика. Применение рекомендованных параметров позволяет защитить информацию, обрабатываемую на клиентских персональных компьютерах (ПК) в организации.

Параметры безопасности разделены на три основных раздела:

1. Политика домена.
2. Политика компьютера.
3. Политика пользователя.

Политика домена

Параметры безопасности, указанные в этом разделе, относятся к домену. Они настраиваются с помощью редактора групповой политики в пространстве имен объекта групповой политики ***Конфигурация компьютера\Конфигурация Windows\Параметры безопасности*** и включают следующие:

1. Параметры политики паролей.
2. Параметры блокировки учетных записей.

Параметры политики 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 2.2).

Таблица 2.2 – Параметры политики паролей, используемые для обеспечения безопасности компьютеров под управлением операционной системы Microsoft® Windows® Vista™ Service Pack 1

Название параметра	**Конфигурация**	**Конфигурация**
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
Принудительно установить журнал паролей	Хранить 24 пароля	Хранить 24 пароля
Хранить пароли, 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 дням*» позволит обеспечить регулярность смены пароля, повышая тем самым безопасность его использования.

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

В конфигурации «Enterprise Client» 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 длинной 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 999 дней. Чтобы разрешить пользователю немедленную смену пароля, используется значение 0.

Параметр безопасности «Принудительно установить журнал паролей» определяет количество новых уникальных паролей, которое необходимо назначить учетной записи пользователя, перед тем как можно будет назначить старый пароль.

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 $1x10^7$ возможных комбинаций. С учетом регистра, количество комбинаций (при использовании только символов латинского алфавита) составляет 52^7. Следовательно, 7-символьный пароль, состоящий только из символов алфавита без знаков пунктуации, с учетом регистра имеет 62^7 комбинаций. При скорости 1 000 000 подстановок в секунду для взлома такого пароля потребуется всего 48 минут. 8-символьный пароль означает $2x10^{11}$ комбинаций. При скорости 1 000 000 подстановок в секунду (показатель многих программ для определения паролей), все возможные комбинации будут проверены через 59 часов. Использование символов, которые вводятся с помощью клавиши ALT, и других специальных символов (например ! или @) значительно увеличивает промежуток времени, необходимый для взлома пароля. Совместное использование описанных символов значительно усложняет осуществление хакерских атак. Поэтому для обеих конфигураций данный параметр безопасности должен иметь значение «*Включен*».

Параметр безопасности «*Хранить пароли, 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). Он также требуется при использовании проверки подлинности в службах IIS. 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 2.3).

Таблица 2.3 – Параметры политики блокировки учетной записи, используемые для обеспечения безопасности компьютеров под управлением операционной системы Microsoft® Windows® Vista™ Service Pack 1

Название параметра	**Конфигурац ия**	**Конфигурац ия**
Длительность блокировка учетных записей	15 минут	15 минут
Пороговое значение блокировки учетных записей	50 неудачных попыток входа в систему	10 неудачных попыток входа в систему

Название параметра	Конфигурация	Конфигурация
Сброс счетчика блокировки через	15 минут	15 минут

Параметр безопасности «Длительность блокировка учетных записей» 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 «Длительность блокировка учетных записей» равным «*15 минут*» обеспечивает достаточную безопасность системы, не вызывая увеличения 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.

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 «*30 минутам*».

В случае, когда клиентский компьютер является автономным компьютером в конфигурациях «Enterprise Client» или «High Security» и функционирует в домене на базе Active Directory или на базе предшествующих версий Windows, параметры политики учетных записей должны определяться для него отдельно от существующей в домене политики учетных записей пользователей.

Политика компьютера

Параметры безопасности, указанные в этом разделе, относятся к компьютерам в домене**.** С помощью редактора групповой политики в пространстве имен объекта групповой политики *Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики* настраиваются:

1. Параметры политики аудита.
2. Параметры назначения прав пользователя.
3. Параметры безопасности.

В пространстве имен объекта групповой политики *Конфигурация компьютера\Конфигурация Windows\Параметры безопасности* настраиваются:

1. Параметры безопасности журнала событий.
2. Параметры брандмауэра Windows в режиме повышенной 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.

WINDOWS® VISTA™ Service Pack 1 включает те же девять параметров политики аудита, что и предыдущие версии Windows: аудит событий входа в систему, аудит управления учетными записями, аудит доступа к службе каталогов, аудит входа в систему, аудит доступа к объектам, аудит изменения политики, аудит использования привилегий, аудит отслеживания процессов, аудит системных событий.

Параметры политики аудита необходимо настроить с помощью редактора групповой политики в пространстве имен объекта групповой политики: *Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Политики аудита* (см.таблицу 2.4).

Таблица 2.4 – Параметры политики аудита, используемые на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Значение	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Аудит событий входа в систему	Успех	Не определен
Аудит управления учетными записями	Успех	Не определен
Аудит доступа к службе каталогов	Не определен	Не определен
Аудит входа в систему	Успех	Не определен
Аудит доступа к объектам	Нет аудита	Не определен
Аудит изменения политики	Успех	Не определен
Аудит использования привилегий	Нет аудита	Не определен
Аудит отслеживания процессов	Нет аудита	Не определен

Для более точного управления политикой аудита WINDOWS® VISTA™ Service Pack 1 предоставляет дополнительные подпараметры политики аудита. Корпорация Microsoft рекомендует использовать в командной строке утилиту *AuditPol.exe*, которая входит в состав операционной системы.

Примечание. Сведения о настройки новых параметров политики аудита представлены в статье 921469 Использование групповой политики для настройки подробных параметров аудита безопасности на клиентских компьютерах с системой WINDOWS® VISTA™ Service Pack 1 в домене Windows Server 2003 или Windows Server 2000 (http://support.microsoft.com/921469).

Параметр политики аудита «*Аудит системных событий*» позволяет регистрировать успешное выполнением и сбои системных событий, к которым относится, например, запуск и завершение работы компьютера, заполнение журналов событий. В таблице 2.5 приведены рекомендуемые подпараметры политики аудита «*Аудит системных событий*»

Таблица 2.5 – Рекомендуемые подпараметры политики аудита «*Аудит системных* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметр	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Расширение системы безопасности	Успех и сбой	Успех и сбой
Целостность системы	Успех и сбой	Успех и сбой
Драйвер IPsec	Успех и сбой	Успех и сбой
Другие системные события	Нет аудита	Нет аудита
Изменение состояния безопасности	Успех и сбой	Успех и сбой

Параметр политики аудита «*Аудит событий входа в систему*» регистрируют события создания и удаления сеансов входа в систему. В таблице 2.6 приведены рекомендуемые подпараметры политики аудита «*Аудит событий входа в систему*»

Таблица 2.6 – Рекомендуемые подпараметры политики аудита «*Аудит событий входа в систему»* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметр	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Вход	Успех	Успех и сбой
Выход	Успех	Успех
Блокировка учетной записи	Нет аудита	Нет аудита
Основной режим IPsec	Нет аудита	Нет аудита

Подпараметр	Конфигурация «Enterprise Client»	Конфигурация «High Security»
Быстрый режим IPsec	Нет аудита	Нет аудита
Расширенный режим IPsec	Нет аудита	Нет аудита
Специальный вход	Успех	Успех
Другие события входа и выхода	Нет аудита	Нет аудита

Параметр политики аудита «*Аудит доступа к объектам*» определяет необходимость аудита событий получении пользователями доступа к объектам (например файлу, папке, разделу реестра или принтеру), для которых задан системный список управления доступом. В таблице 2.7 приведены рекомендуемые подпараметры политики аудита «*Аудит событий входа в систему*»

Таблица 2.7 – Рекомендуемые подпараметры политики аудита «*Аудит доступа к объектам»* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметры	Конфигурация «Enterprise Client»	Конфигурация «High Security»
Файловая система	Нет аудита	Сбой
Реестр	Нет аудита	Сбой
Объект ядра	Нет аудита	Нет аудита
SAM	Нет аудита	Нет аудита
Службы сертификатов	Нет аудита	Нет аудита
Создано приложением	Нет аудита	Нет аудита
Использование дескриптора	Нет аудита	Нет аудита
Общая папка	Нет аудита	Нет аудита
Отбрасывание пакетов платформой фильтрации	Нет аудита	Нет аудита
Подключение платформы фильтрации	Нет аудита	Нет аудита
Другие события доступа к объекту	Нет аудита	Нет аудита

Параметр политики аудита «*Аудит использования привилегий*» определяет необходимость выполнения аудита для всех случаев применения прав пользователя. В

таблице 2.8 приведены рекомендуемые подпараметры политики аудита «*Аудит использования привилегий*»

Таблица 2.8 – Рекомендуемые подпараметры политики аудита «*Аудит использования привилегий»* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметры	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Использование прав, затрагивающих конфиденциальные данные	Нет аудита	Успех и сбой
Использование прав, не затрагивающеих конфиденциальные данные	Нет аудита	Нет аудита
Другие события, связанные с использованием привилегии	Нет аудита	Нет аудита

Параметр политики аудита «*Аудит отслеживания процессов*» определяет необходимость выполнения аудита таких процессов, как активация программ, завершение процессов, дублирование дескрипторов. В таблице 2.9 приведены рекомендуемые подпараметры политики аудита «*Аудит использования привилегий*»

Таблица 2.9 – Рекомендуемые подпараметры политики аудита «*Аудит отслеживания процессов»* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметры	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Завершение процесса	Нет аудита	Нет аудита
Действие DPAPI	Нет аудита	Нет аудита
События RPC	Нет аудита	Нет аудита
Создание процессов	Успех	Успех

Параметр политики аудита «*Аудит изменения политики*» определяет необходимость выполнения аудита всех изменений прав пользователя, политик безопасности брандмауэра и

самой политики аудита. В таблице 2.10 приведены рекомендуемые подпараметры политики аудита «*Аудит изменения политик*»

Таблица 2.10 – Рекомендуемые подпараметры политики аудита «*Аудит изменения политик»* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметры	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Изменение политики аудита	Успех и сбой	Успех и сбой
Изменение политики проверки подлинности	Успех	Успех
Изменение политики авторизации	Нет аудита	Нет аудита
Изменение политики на уровне правила MPSSVC	Нет аудита	Нет аудита
Изменение политики платформы фильтрации	Нет аудита	Нет аудита
Другие события изменения политики	Нет аудита	Нет аудита

Параметр политики аудита «*Аудит управления учетными данными*» позволяет отслеживать попытки создания учетных записей пользователей или групп, их изменение, включения или отключения учетных записей пользователей, изменения паролей пользователей и включения аудита для событий управления учетными записями. В таблице 2.11 приведены рекомендуемые подпараметры политики аудита «*Аудит управления учетными данными*»

Таблица 2.11 – Рекомендуемые подпараметры политики аудита «*Аудит управления учетными данными»* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметры	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Управление учетными записями	Успех	Успех и сбой
Управление учетными записями компьютера	Успех	Успех и сбой
Управление группами безопасности	Успех	Успех и сбой
Управление группами рассылки	Нет аудита	Нет аудита

Подпараметры	Конфигурация «Enterprise Client»	Конфигурация «High Security»
Управление группами пользователей приложения	Нет аудита	Нет аудита
Другие события управления учетными записями	Успех	Успех и сбой

.

Параметр политики аудита «*Аудит доступа к службе каталогов*» относится только к контроллерам домена. В таблице 2.12 приведены рекомендуемые подпараметры политики аудита «*Аудит управления учетными данными*»

Таблица 2.12 – Рекомендуемые подпараметры политики аудита «*Аудит доступа к службе каталогов»* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметры	Конфигурация «Enterprise Client»	Конфигурация «High Security»
Изменения службы каталогов	Нет аудита	Нет аудита
Репликация службы каталогов	Нет аудита	Нет аудита
Подробная репликация службы каталогов	Нет аудита	Нет аудита
Доступ к службе каталогов	Нет аудита	Нет аудита

Параметр политики аудита «*Аудит входа в систему*» позволяет отслеживать события, связанные с проверкой учетных данных. В таблице 2.13 приведены рекомендуемые подпараметры политики аудита «*Аудит входа в систему*»

Таблица 2.13 – Рекомендуемые подпараметры политики аудита «*Аудит входа в систему»* для использования на компьютерах под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Подпараметры	Конфигурация «Enterprise Client»	Конфигурация «High Security»
Проверка учетных данных	Успех	Успех и сбой
События билетов	Нет аудита	Нет аудита
Другие события входа под учетной записью	Нет аудита	Нет аудита

Параметры назначения прав пользователей

Задачи, которые пользователь имеет право выполнять в домене или в операционной системе, установленной на компьютере, называются правами пользователя.

В операционной системе WINDOWS® VISTA™ Service Pack 1 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 2.14 – Параметры назначения прав пользователей, используемые для обеспечения безопасности компьютеров под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Название параметра	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Доступ к компьютеру из сети	"Администраторы", "Пользователи"	"Администраторы"
Работать в режиме операционной системы	Никто	Никто
Настраивать квоты памяти для процесса	Не определен	"Администраторы", "Локальная служба", "Сетевая служба"
Локальный вход в систему	"Администраторы", "Пользователи"	"Администраторы", "Пользователи"
Разрешать вход в систему через службу терминалов	Не определен	Никто
Архивация файлов и каталогов	Не определен	"Администраторы"
Обход перекрестной проверки	Не определен	"Администраторы", "Пользователи", "Локальная служба", "Сетевая служба"
Изменение системного времени	"Локальная служба", "Администраторы"	"Локальная служба", "Администраторы"
Изменение часового пояса	Не определен	"Локальная служба", "Администраторы", "Пользователи"

Название параметра	Конфигурация «Enterprise Client»	Конфигурация «High Security»
Создание файла подкачки	"Администраторы"	"Администраторы"
Создание постоянных общих объектов	Не определен	Никто
Создание маркерного объекта	Не определен	Никто
Создание глобальных объектов	Не определен	"Администраторы", "Служба", "Локальная служба", "Сетевая служба"
Создание символических ссылок	Не определен	"Администраторы"
Отладка программ	"Администраторы"	Никто
Отказ в доступе к компьютеру из сети	"Гости"	"Гости"
Отказ во входе в качестве пакетного задания	Не определен	"Гости"
Отклонить локальный вход	"Гости"	"Гости"
Запретить вход в систему через службу терминалов	Не определен	"Все"
Разрешить делегирование для учетных записей компьютеров и пользователей	Не определен	Никто

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, NetBIOS, CIFS, и COM+.

Параметр «*Работать в режиме операционной системы*» позволяет процессу получать доступ к ресурсам, для которых разрешен доступ пользователю.

Параметр «*Настраивать квоты памяти для процесса*» позволяет пользователю настраивать максимальный размер памяти для процесса.

Параметр «*Локальный вход в систему*» определяет, какие пользователи могут интерактивно входить в систему. Этот право требуется для входа пользователей в

клиентский компьютер с использованием сочетания клавиш CTRL+ALT+DEL на клавиатуре или с помощью служб терминалов.

Параметр «*Разрешать вход в систему через службу терминалов*» определяет, какие пользователи или группы пользователей имеют право входить в систему в качестве клиента службы терминалов.

Параметр «*Архивация файлов и каталогов*» позволяет пользователям обходить разрешения на архивацию для файлов и каталогов при резервном копировании системы.

Параметр «*Обход перекрестной проверки*» определяет пользователей, которые могут выполнять обзор каталогов в файловой системе NTFS или реестре, не имея специального разрешения на доступ "Обзор папок".

Параметр «*Изменение системного времени*» определяет, каким пользователям и группам пользователей разрешено изменять время и дату на внутренних часах компьютеров.

Параметр «*Изменение часового пояса*» определяет, какие пользователи могут изменять часовой пояс на компьютере. Эта возможность не представляет опасности для компьютера и может быть полезна мобильным сотрудникам.

Параметр «*Создание файла подкачки*» позволяет пользователям изменять размер файла подкачки. Чрезмерно увеличив или уменьшив размер файла подкачки, злоумышленник может легко воздействовать на производительность атакуемого компьютера.

Параметр «*Создание постоянных общих объектов*» позволяет пользователям создавать объекты каталогов в диспетчере объектов. Это право пользователя является полезным для компонентов режима ядра, которые расширяют пространство имен объекта.

Параметр «*Создание маркерного объекта*» разрешает процессу создавать маркер доступа, который может предоставлять повышенные права для доступа к конфиденциальным данным. В средах, для которых безопасность очень важна, запрещено назначать это право пользователям.

Параметр «*Создание глобальных объектов*» определяет, могут ли пользователи создавать глобальные объекты, доступные во всех сеансах. Пользователи, не имеющие этого права, могут создавать объекты для своих сеансов. Пользователи, имеющие право на создание глобальных объектов, могут влиять на процессы, которые запускаются в сеансах других пользователей.

Параметр «*Создание символических ссылок*» определяет, какие пользователи могут создавать символические ссылки. В WINDOWS® VISTA™ Service Pack 1 к объектам файловой системы NTFS, таким как файлы и папки, можно получить доступ с помощью нового типа объектов файловой системы — символических ссылок. Символическая ссылка — это указатель (как ярлык или LNK-файл) на другой объект файловой системы, которым может быть файл, папка, ярлык или другая символическая ссылка. Различие между ярлыком и символической ссылкой заключается в том, что ярлык работает только в оболочке Windows. Для других программ и приложений ярлыки являются обычными файлами, тогда

как символическая ссылка — это возможность файловой системы NTFS. Символические ссылки потенциально могут открывать доступ к уязвимостям в приложениях, которые не рассчитаны на их использование.

Параметр «*Отладка программ*» определяет, какие пользователи будут иметь право применять отладчик к любому процессу или ядру, что обеспечивает полный доступ к уязвимым или критически важным компонентам операционной системы. SSLF.

Параметр «*Отказ в доступе к компьютеру из сети*» запрещает пользователям выполнять подключение к компьютеру из сети, при котором возможен удаленный доступ к данным и их изменение.

Параметр «*Отказ во входе в качестве пакетного задания*» запрещает вход пользователей в систему с помощью средства пакетной очереди — возможности Windows Server 2003, которая используется для задания расписания автоматического однократного или многократного выполнения задач.

Параметр «*Отклонить локальный вход*» запрещает пользователям локальный вход в компьютера. Если пользователи, не имеющие соответствующих полномочий, войдут локально в систему, они могут загрузить вредоносные программы или повысить свои привилегии на компьютере.

Параметр «*Запретить вход в систему через службу терминалов*» запрещает пользователям входить в систему с помощью подключения к удаленному рабочему столу.

Параметр «Разрешить делегирование для учетных записей компьютеров и пользователей» разрешает пользователям изменять значение параметра *Делегирование разрешено* для объекта компьютера в Active Directory.

В таблице 2.15 указаны рекомендуемые значения для второй группы параметров назначения прав пользователя.

Таблица 2.15 – Параметры назначения прав пользователей, используемые для обеспечения безопасности компьютеров под управлением операционной системы WINDOWS® VISTA™ Service Pack 1

Название параметра	**Конфигурация «Enterprise Client»**	**Конфигурация «High Security»**
Принудительное завершение работы из удаленной системы	"Администраторы"	"Администраторы"
Создание аудита безопасности	"Локальная служба", "Сетевая служба"	"Локальная служба", "Сетевая служба"
Имитация клиент после проверки подлинности	Не определен	"Администраторы", "Служба", "Локальная служба", "Сетевая служба"

Название параметра	Конфигурация «Enterprise Client»	Конфигурация «High Security»
Увеличение рабочего множества процесса	Не определен	Администраторы
Увеличение приоритета выполнения	Администраторы	Администраторы
Загрузка и выгрузка драйверов устройств	Администраторы	Администраторы
Блокировка страниц в памяти	Никто	Никто
Вход в систему в качестве пакетного задания	Не определен	Никто
Вход в качестве службы	Не определен	Никто
Управление журналом аудита и безопасности	Администраторы	Администраторы
Изменение параметров среды изготовителем	Администраторы	Администраторы
Выполнение задач обслуживания томов	Администраторы	Администраторы
Конфигурация отдельного процесса	Не определен	Администраторы
Конфигурация производительности системы	Администраторы	Администраторы
Удаление компьютера из стыковочного узла	Администрация, пользователи	Администрация, пользователи
Замена маркера уровня процесса	Локальная служба, сетевая служба	Локальная служба, сетевая служба
Восстановление файлов и каталогов	Не определен	Администраторы
Завершение работы системы	Администрация, пользователи	Администрация, пользователи
Стать владельцем файлов или других объектов	Администраторы	Администраторы

Параметр *«Принудительное завершение работы с удаленного компьютера»* позволяет пользователям отключать компьютеры с операционной системой WINDOWS® VISTA™ Service Pack 1 с удаленных компьютеров в сети. Любой обладающий этим правом

пользователя может вызвать отказ в обслуживании, что приведет к тому, что компьютер не сможет обрабатывать запросы пользователей.

Параметр «*Создание записей аудита безопасности*» определяет, какие пользователи или процессы могут создавать записи аудита в журнале безопасности.

Параметр *«Увеличение рабочего множества процесса»* определяет, какие учетные записи пользователей могут увеличивать или уменьшать размер рабочего множества процесса. Рабочее множество процесса — это множество страниц памяти, видимых в текущий момент процессу в физической оперативной памяти. Эти страницы являются резидентными, и их использование приложением не приведет к ошибке доступа.

Параметр «*Увеличение приоритета процесса*» позволяет пользователям изменять приоритет процессора.

Параметр «*Загрузка и выгрузка драйверов устройств*» разрешает пользователям динамически загружать в систему новый драйвер устройства..

Параметр «*Блокировка страниц в памяти*» позволяет процессу хранить данные в физической памяти, что предотвращает сброс данных в страницы виртуальной памяти на диск.

Параметр «*Вход в систему в качестве пакетного задания*» разрешает пользователям входить в систему, используя службу планировщика заданий.

Параметр «*Вход в качестве службы*» разрешает запускать сетевые службы или регистрировать процесс как службу, запускаемую в системе.

Параметр «*Управление журналом аудита и безопасности*» определяет, какие пользователи могут изменять параметры аудита для файлов и каталогов и очищать журнал безопасности.

Параметр *«Изменение переменных окружения, заданных изготовителем»* позволяет пользователям настраивать системные переменные окружения, влияющие на конфигурацию оборудования. Эти данные обычно хранятся в последней удачной конфигурации руководстве.

Параметр *«Выполнение задач обслуживания томов* позволяет пользователям управлять конфигурацией системного тома или диска, что позволяет пользователю удалить том и может привести к потере данных, а также к отказу в обслуживании.

Параметр *«Конфигурация отдельного процесса»* определяет, каким пользователям разрешено использовать средства для наблюдения за производительностью несистемных процессов. Как правило, не требуется настраивать это право пользователя на использование оснастки "Производительность" консоли управления (MMC). Тем не менее, это право необходимо использовать в случае, если системный монитор настроен на сбор данных с помощью инструментария управления Windows (WMI).

Параметр *«Конфигурация производительности системы»* позволяет пользователям использовать средства для просмотра производительности различных системных процессов,

а эти сведения могут быть использованы злоумышленниками для определения активных системных процессов и подготовки площадки для атаки на компьютер.

Параметр «Удаление компьютера из стыковочного узла» параметр политики позволяет пользователю портативного компьютера выбрать пункт *Извлечь компьютер* в меню *Пуск*, чтобы отстыковать компьютер.

Параметр *«Замена маркера уровня процесса»* позволяет одному процессу или службе запускать другую службу или процесс с другим маркером доступа к системе безопасности, который можно использовать для изменения маркера доступа к системе безопасности этого дочернего процесса и повышения полномочий.

Параметр *«Восстановление файлов и каталогов»* определяет, каким пользователям разрешено обходить разрешения для файлов, каталогов, реестра и других постоянных объектов при восстановлении из резервных копий файлов и каталогов на компьютере с операционной системой WINDOWS® VISTA™ Service Pack 1 .

Параметр *«Завершение работы системы»* определяет, каким пользователям, локально вошедшим в систему, разрешено завершать работу операционной системы с помощью команды "Завершить работу".

Параметр «*Стать владельцем файлов или других объектов*» позволяет пользователям становиться владельцами файлов, папок, разделов реестра, процессов или потоков и обходить все разрешения, действующие для защиты объектов.

2.3Последовательность действий по настройке сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1

Общие указания по настройке параметров безопасности сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1

Для настройки параметров безопасности клиентского компьютера под управлением операционной системы WINDOWS® VISTA™ Service Pack 1 , являющегося членом домена Active Directory, в соответствии с конфигурациями «Enterprise» или «High Security» необходимо использовать только объекты групповой политики. Шаблоны безопасности можно применять для настройки параметров безопасности автономного клиентского компьютера.

Для упрощения настройки параметров безопасности необходимо загрузить сценарий GPOAccelerator.wsf из Центра загрузки Microsoft (http://*www.microsoft.com*) и установить на компьютере. После установки сценарий находится в папке WINDOWS® VISTA™ Service Pack 1 Security Guide\GPOAccelerator Tool. Он обеспечивает автоматическое создание объектов групповой политики и связывает их с соответствующими подразделениями в среде.

Для клиентских компьютеров в среде «Enterprise Client» создаются следующие четыре объекта групповой политики:

VSG EC Domain Policy для домена;

VSG EC Users Policy для пользователей;

VSG EC Desktop Policy для настольных компьютеров;

VSG EC Laptop Policy для переносных компьютеров.

Для клиентских компьютеров в среде «High Security» создаются следующие четыре объекта групповой политики:

VSG SSLF Domain Policy для домена;

VSG SSLF Users Policy для пользователей;

VSG SSLF Desktop Policy для настольных компьютеров;

VSG SSLF Laptop Policy для переносных компьютеров.

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

Для настройки необходимо:

1. Создать объекты групповой политики для конфигурации «Enterprise Client».
2. Используя консоль управления групповыми политиками связать политики VSG EC Domain Policy с доменом.
3. Используя консоль управления групповыми политиками проверить результаты.

Для создания объектов групповой политики следует:

- войти с учетной записью администратора домена в компьютер под управлением WINDOWS® VISTA™ Service Pack 1 ;
- нажать кнопку ***Пуск*** и выбрать пункты ***Все программы*** и ***Windows Vista Security Guide***;
- открыть папку ***GPOAccelerator Tool\Security Group Policy Objects***;
- щелкнуть правой кнопкой мыши файл ***Command-line Here.cmd*** и выбрать пункт ***Запуск от имени администратора***, чтобы открыть командную строку с привилегиями администратора домена;
- в командной строке ввести ***cscript GPOAccelerator.wsf /Enterprise*** и нажать клавишу ***ВВОД***;
- в окне с сообщением ***Click Yes to continue, or No to exit the script*** нажать кнопку ***Да***, чтобы продолжить, или для выхода ***Нет***;
- в окне с сообщением ***The SSLF GPOs are created*** нажать кнопку **OK**.

Для проверки результатов создания объектов групповой политики:

- Нажмите кнопку **Пуск** системы WINDOWS® VISTA™ Service Pack 1 , выберите пункты **Все программы**, **Стандартные** и **Выполнить**;

- В поле **Открыть** введите **gpmc.msc** и нажмите кнопку **ОК**;
- Щелкните нужный лес, выберите пункт **Domains** (Домены) и домен;
- Разверните узел **Group Policy Objects** (Объекты групповой политики) и убедитесь в том, что четыре созданных объекта групповой политики VSG EC соответствуют объектам на рисунке 1.

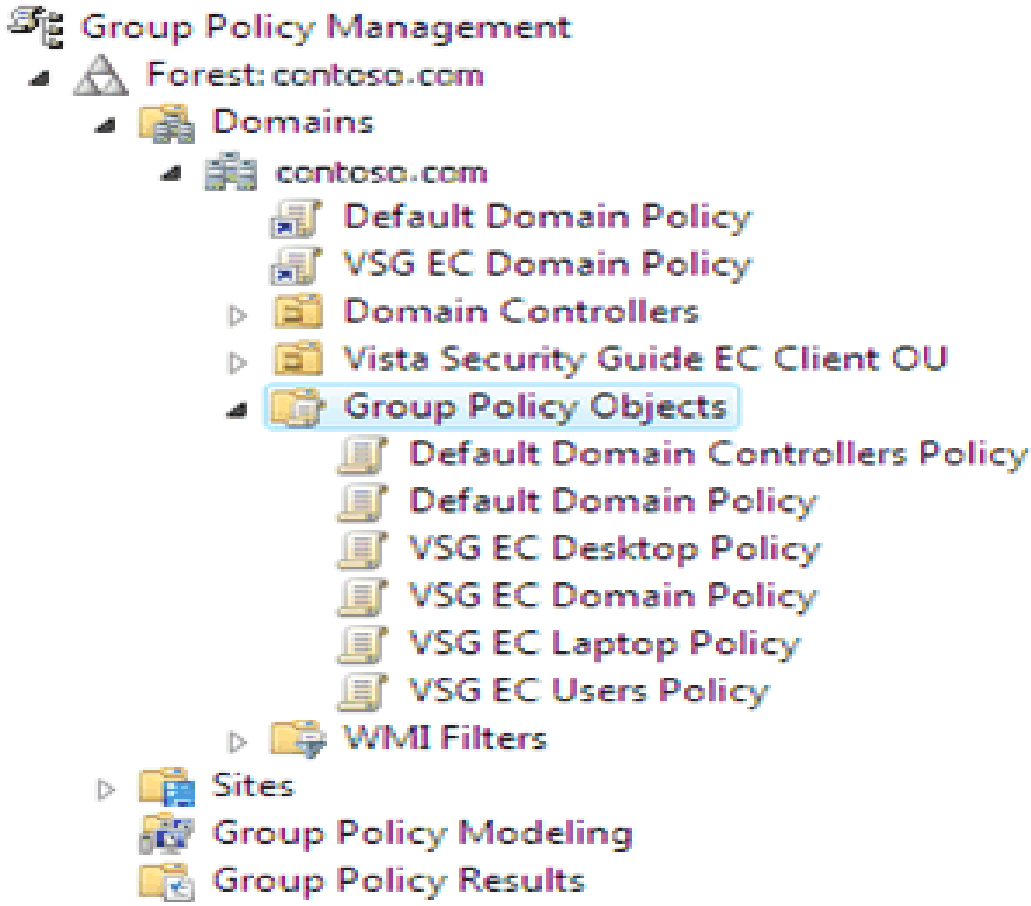

Рис.1

Для связи объектов групповой политики с подразделениями необходимо выполнить следующие операции:

- нажать кнопку ***Пуск*** системы WINDOWS® VISTA™ Service Pack 1 , и выбрать пункты ***Все программы***, ***Стандартные*** и ***Выполнит***;
- в поле ***Открыть*** введите ***gpmc.msc*** и нажать кнопку ***ОК***;
- в дереве ***Domains*** (Домены) щелкнуть домен правой кнопкой мыши и выбрать пункт ***Link an existing GPO*** (Связать существующий объект групповой политики);
- в диалоговом окне ***Select GPO*** (Выбор объекта групповой политики) выбрать объект групповой политики ***VSG EC Domain Policy*** (Политика домена VSG EC) и нажать кнопку ***ОК***;

- в области сведений выбрать пункт ***VSG EC Domain Policy*** (Политика домена VSG EC) и нажать кнопку ***Move link to top*** (Переместить ссылку наверх);
- Щелкнуть правой кнопкой мыши узел WINDOWS® VISTA™ Service Pack 1 Users OU (Подразделение пользователей WINDOWS® VISTA™ Service Pack 1) и выбрать пункт **Link an existing GPO** (Связать существующий объект групповой политики).
- В диалоговом окне **Select GPO** (Выбор объекта групповой политики) выбрать объект групповой политики **VSG EC Users Policy** (Политика пользователей VSG EC) и нажать кнопку **OK**.
- Щелкнуть правой кнопкой мыши узел **Desktop OU** (Подразделение настольных компьютеров) и выбрать пункт **Link an existing GPO** (Связать существующий объект групповой политики).
- В диалоговом окне **Select GPO** (Выбор объекта групповой политики) выбрать объект групповой политики **VSG EC Desktop Policy** (Политика настольных компьютеров VSG EC) и нажать кнопку **OK**.
- Щелкнуть правой кнопкой мыши узел **Laptop OU** (Подразделение переносных компьютеров) и выбрать пункт **Link an existing GPO** (Связать существующий объект групповой политики).
- В диалоговом окне **Select GPO** (Выбор объекта групповой политики) выбрать объект групповой политики **VSG EC Laptop Policy** (Политика переносных компьютеров VSG EC) и нажать кнопку **OK**.
- Повторить эти действия для всех других созданных подразделений пользователей или компьютеров, чтобы связать их с соответствующими объектами групповой политики.

Чтобы подтвердить связи объектов групповой политики с помощью консоли управления групповыми политиками следует развернуть узел ***Group Policy Objects*** (Объекты групповой политики) и выбрать объект групповой политики. В области сведений открыть вкладку ***Scope*** (Область) и просмотреть сведения в столбцах ***Link Enabled*** (Связь включена) и ***Path*** (Путь).

Настройка автономного клиентского компьютера в конфигурации «Enterprise Client»

Для настройки локальной политики безопасности на автономных клиентских компьютерах в конфигурации «Enterprise Client» возможно использовать шаблоны безопасности, устанавливаемые на компьютер вместе со сценарием GPOAccelerator.wfs,

который упрощает применение шаблонов. Для этого необходимо выполнить следующие операции:

- войти в компьютер под управлением WINDOWS® VISTA™ Service Pack 1 с учетной записью администратора;
- нажать кнопку ***Пуск*** системы WINDOWS® VISTA™ Service Pack 1 , выбрать пункты ***Все программы*** и ***Windows Vista Security Guide***;
- открыть папку ***GPOAccelerator Tool\Security Group Policy Objects***;
- щелкнуть правой кнопкой мыши файл ***Command-line Here.cmd*** и выбрать пункт ***Запуск от имени администратора***, чтобы открыть командную строку со всеми привилегиями администратора;
- в командной строке ввести ***cscript GPOAccelerator.wsf /Enterprise /Desktop*** или ***cscript GPOAccelerator.wsf /Enterprise /Laptop*** и нажать клавишу ***ВВОД***.

Эта процедура изменяет параметры локальной политики безопасности, используя значения в шаблонах безопасности для конфигурации «Enterprise Client».

Настройка клиентского компьютера, являющегося членом домена Active Directory, в конфигурации «High Security»

Для настройки необходимо:

1. Создать объекты групповой политики для конфигурации «High Security».
2. Используя консоль управления групповыми политиками связать политики VSG EC Domain Policy с доменом.
3. Используя консоль управления групповыми политиками проверить результаты.

Для создания объектов групповой политики следует:

- войти с учетной записью администратора домена в компьютер под управлением WINDOWS® VISTA™ Service Pack 1 ;
- нажать кнопку ***Пуск*** и выбрать пункты ***Все программы*** и ***Windows Vista Security Guide***;
- открыть папку ***GPOAccelerator Tool\Security Group Policy Objects***;
- щелкнуть правой кнопкой мыши файл ***Command-line Here.cmd*** и выбрать пункт ***Запуск от имени администратора***, чтобы открыть командную строку с привилегиями администратора домена;
- в командной строке ввести ***cscript GPOAccelerator.wsf / SSLF*** и нажать клавишу ***ВВОД***;
- в окне с сообщением ***Click Yes to continue, or No to exit the script*** нажать кнопку ***Да***, чтобы продолжить, или для выхода ***Нет***;
- в окне с сообщением ***The SSLF GPOs are created*** нажать кнопку **OK**.

Для проверки результатов создания объектов групповой политики:

- Нажать кнопку **Пуск** системы WINDOWS® VISTA™ Service Pack 1 , выбрать пункты **Все программы**, **Стандартные** и **Выполнить**;
- В поле **Открыть** ввести **gpmc.msc** и нажать кнопку **ОК**;
- Щелкнуть нужный лес, выбрать пункт **Domains** (Домены) и домен;
- Развернуть узел **Group Policy Objects** (Объекты групповой политики) и убедиться в том, что четыре созданных объекта групповой политики VSG EC соответствуют объектам на рисунке 2.

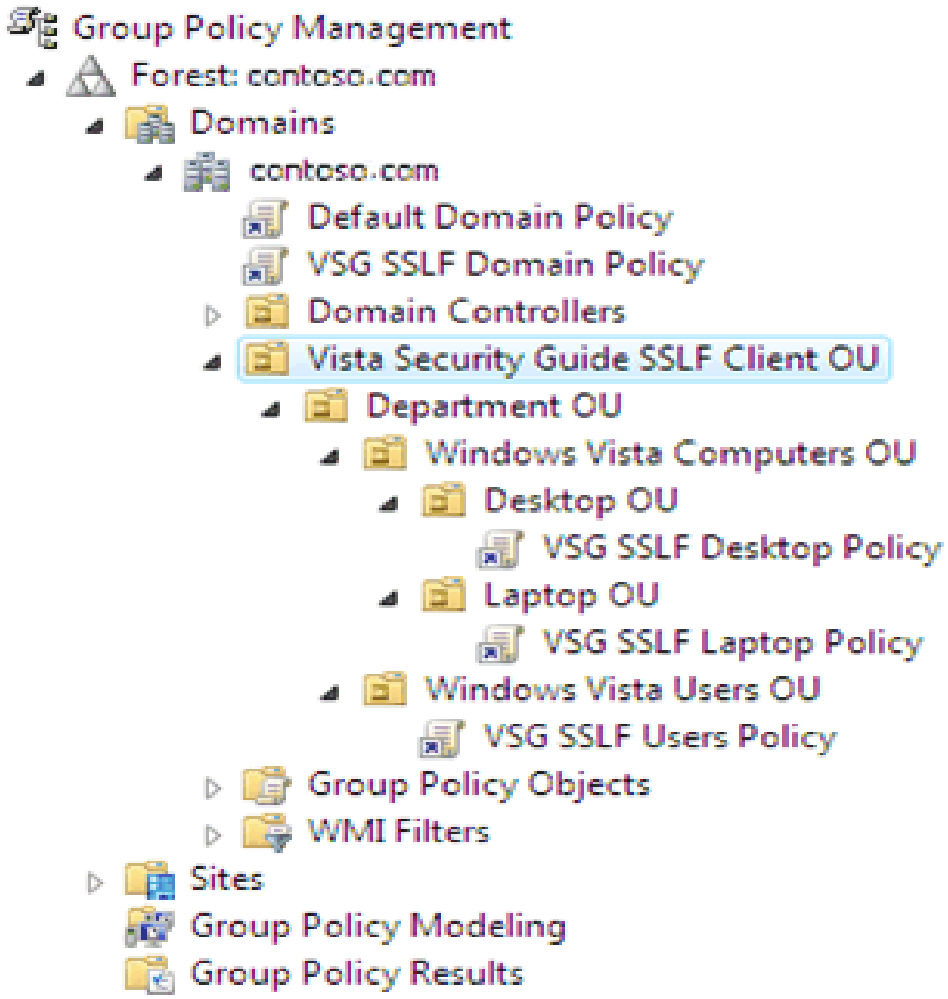

Рис.2

Для связи объектов групповой политики с подразделениями необходимо выполнить следующие операции:

- нажать кнопку ***Пуск*** системы WINDOWS® VISTA™ Service Pack 1 , и выбрать пункты ***Все программы***, ***Стандартные*** и ***Выполнит***;
- в поле ***Открыть*** введите ***gpmc.msc*** и нажать кнопку ***ОК***;

- в дереве ***Domains*** (Домены) щелкнуть домен правой кнопкой мыши и выбрать пункт ***Link an existing GPO*** (Связать существующий объект групповой политики);
- в диалоговом окне ***Select GPO*** (Выбор объекта групповой политики) выбрать объект групповой политики ***VSG SSLF Domain Policy*** (Политика домена VSG EC) и нажать кнопку ***OK***;
- в области сведений выбрать пункт ***VSG SSLF Domain Policy*** (Политика домена VSG EC) и нажать кнопку ***Move link to top*** (Переместить ссылку наверх);
- Щелкнуть правой кнопкой мыши узел Windows Vista Users OU (Подразделение пользователей WINDOWS® VISTA™ Service Pack 1) и выбрать пункт ***Link an existing GPO*** (Связать существующий объект групповой политики).
- В диалоговом окне ***Select GPO*** (Выбор объекта групповой политики) выбрать объект групповой политики ***VSG SSLF Users Policy*** (Политика пользователей VSG EC) и нажать кнопку **OK**.
- Щелкнуть правой кнопкой мыши узел ***Desktop OU*** (Подразделение настольных компьютеров) и выбрать пункт ***Link an existing GPO*** (Связать существующий объект групповой политики).
- В диалоговом окне ***Select GPO*** (Выбор объекта групповой политики) выбрать объект групповой политики ***VSG SSLF Desktop Policy*** (Политика настольных компьютеров VSG EC) и нажать кнопку **OK**.
- Щелкнуть правой кнопкой мыши узел ***Laptop OU*** (Подразделение переносных компьютеров) и выбрать пункт ***Link an existing GPO*** (Связать существующий объект групповой политики).
- В диалоговом окне ***Select GPO*** (Выбор объекта групповой политики) выбрать объект групповой политики ***VSG SSLF Laptop Policy*** (Политика переносных компьютеров VSG SSLF) и нажать кнопку **OK**.
- Повторить эти действия для всех других созданных подразделений пользователей или компьютеров, чтобы связать их с соответствующими объектами групповой политики.

Чтобы подтвердить связи объектов групповой политики с помощью консоли управления групповыми политиками следует развернуть узел ***Group Policy Objects*** (Объекты групповой политики) и выбрать объект групповой политики. В области сведений открыть вкладку ***Scope*** (Область) и просмотреть сведения в столбцах ***Link Enabled*** (Связь включена) и ***Path*** (Путь).

Настройка автономного клиентского компьютера в конфигурации «High Security»

Для настройки локальной политики безопасности на автономных клиентских компьютерах в конфигурации «High Security» возможно использовать шаблоны безопасности, устанавливаемые на компьютер вместе со сценарием GPOAccelerator.wfs, который упрощает применение шаблонов. Для этого необходимо выполнить следующие операции:

- войти в компьютер под управлением WINDOWS® VISTA™ Service Pack 1 с учетной записью администратора;
- нажать кнопку ***Пуск*** системы WINDOWS® VISTA™ Service Pack 1 , выбрать пункты ***Все программы*** и ***Windows Vista Security Guide***;
- открыть папку ***GPOAccelerator Tool\Security Group Policy Objects***;
- щелкнуть правой кнопкой мыши файл ***Command-line Here.cmd*** и выбрать пункт ***Запуск от имени администратора***, чтобы открыть командную строку со всеми привилегиями администратора;
- в командной строке ввести ***cscript GPOAccelerator.wsf /SSLF /Desktop*** или ***cscript GPOAccelerator.wsf /SSLF /Laptop*** и нажать клавишу ***ВВОД***.

Эта процедура изменяет параметры локальной политики безопасности, используя значения в шаблонах безопасности для конфигурации «High Security».

3 Контроль сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1

3.1 Контроль маркирования сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1

Контроль маркирования сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1 в совокупности с контролем исходного состояния, основанном на контрольном суммировании, направлен на получение удостоверения в том, что на рабочей станции установлена сертифицированная версия операционной системы WINDOWS® VISTA™ Service Pack 1 .

Контроль маркирования проводится следующим образом:

1. Удостовериться, что на упаковочной коробке дистрибутива операционной системы, установленной на рабочей станции, присутствует надпись WINDOWS® VISTA™ Service Pack 1 .
2. Удостовериться, что упаковочная коробка дистрибутива операционной системы, установленной на рабочей станции, маркирована знаком соответствия сертифицированной продукции.
3. Удостовериться, что на оптическом носителе дистрибутива операционной системы, установленной на рабочей станции, присутствует надпись WINDOWS® VISTA™ Service Pack 1 .
4. Удостовериться, что загрузка операционной системы, установленной на рабочей станции, сопровождается надписью WINDOWS® VISTA™ Service Pack 1 .

3.2 Порядок проверки соответствия текущих значений параметров безопасности значениям, установленным в шаблонах безопасности

Для проверки соответствия текущих параметров безопасности групповой политики параметрам безопасности, определенным в соответствующем шаблоне (соответствующих шаблонах) безопасности, необходимо выполнить анализ безопасности операционной системы WINDOWS® VISTA™ Service Pack 1 .

Анализ безопасности системы с использование интерфейса Windows

Для анализа безопасности системы необходимо выполнить следующие действия:

1.Открыть 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:

- 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 необходимых шаблонов безопасности и нажать кнопку «Открыть»;
- чтобы открыть существующую базу данных, необходимо выбрать базу данных и нажать кнопку «Открыть».

4.Посредством контекстного меню выбрать пункт «Импорт политики» и последовательно импортировать соответствующие шаблоны безопасности, 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 необходим в случае импортирования двух различных шаблонов безопасности (например, шаблонов VSG EC Domain.inf и VSG ES Desktop.inf), которые в дальнейшем будут использоваться для анализ 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 «Анализ компьютера».

6.Выполнить одно из следующих действий:

- для использования стандартного журнала в группе «Путь файла журнала ошибок» нажать кнопку «ОК»;
- для выбора другого журнала ввести в поле «Путь файла журнала ошибок» допустимое путь и имя файла.

7.По завершении анализа безопасности компьютера просмотреть файл журнала (чтобы просмотреть файл журнала необходимо посредством нажатия правой кнопкой мыши узла «Анализ и настройка безопасности» выбрать команду «Просмотреть файл журнала») или результаты анализа на предмет несовпадения параметров безопасности. Если элемент определен

в шаблоне безопасности и в системе, однако значения параметров безопасности не совпадают, то в файле журнала данный элемент будет отмечен строкой «Не соответствует - <*Наименование_параметра*>, а в результатах анализа помечен знаком .

8.Закрыть оснастку «Анализ и настройка безопасности».

3.3Автоматизированный контроль сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1

Для контроля версии и настроек безопасности операционной системы WINDOWS® VISTA™ Service Pack 1 может использоваться «Программа контроля сертифицированной версии ОС WINDOWS® VISTA™ Service Pack 1 , поставляемая дополнительно к дистрибутиву на компакт-диске. Установка программы осуществляется путем копирования каталога VistaCheck на жесткий магнитный диск ПЭВМ. Запуск программы на исполнение осуществляется путем выбора исполняемого файла VistaCheck.exe и двойного щелчка левой кнопкой мыши на его пиктограмме.

В случае, если версия операционной системы соответствует сертифицированной, появившееся окно должно иметь вид, представленный на рисунке 3.

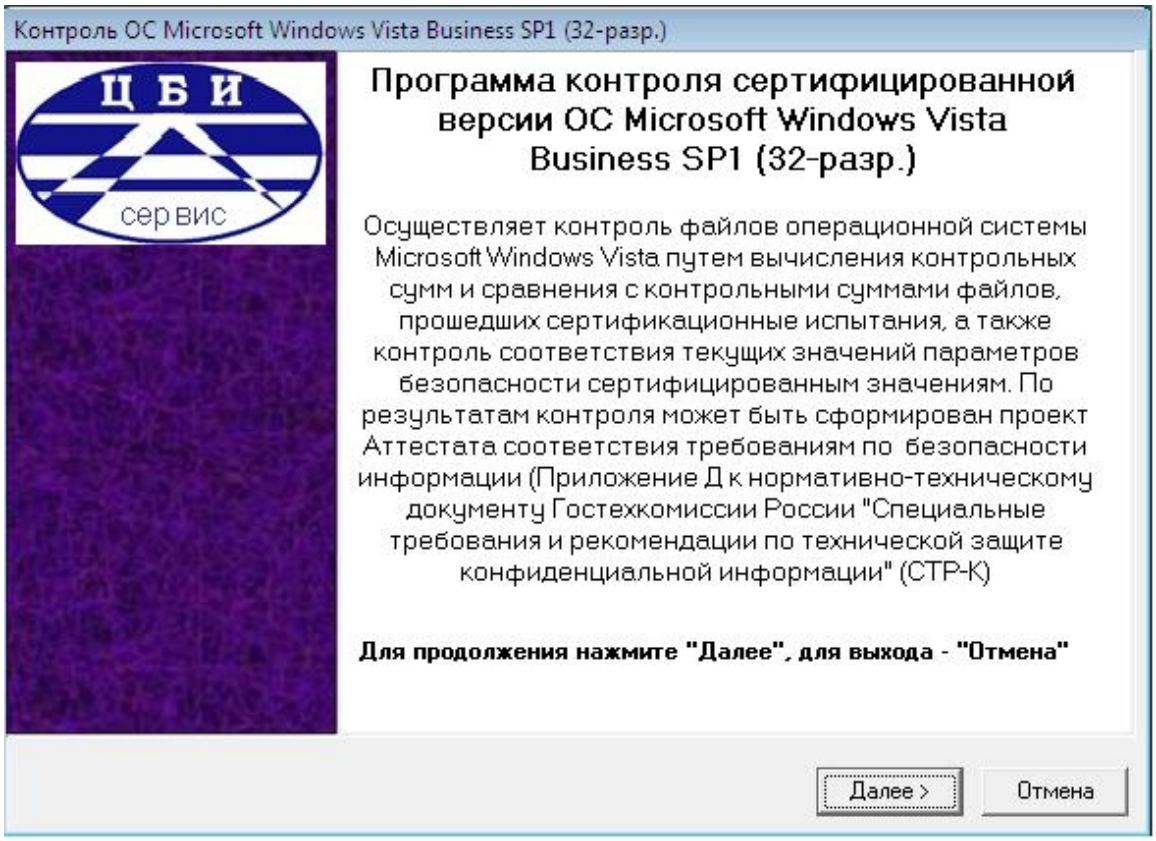

Рисунок 3 – Вид окна программы контроля сертифицированной версии ОС WINDOWS® VISTA™ Service Pack 1 после запуска исполняемого файла VistaCheck.exe

В появившемся после запуска окне необходимо нажать кнопку «Далее». После этого должен начаться контроль соответствия файлов и настроек безопасности текущей версии операционной системы и версии операционной системы WINDOWS® VISTA™ Service Pack 1 , прошедшей сертификационные испытания. После успешного завершения контроля соответствия файлов и настроек окно программы должно иметь вид, представленный на рисунке 4.

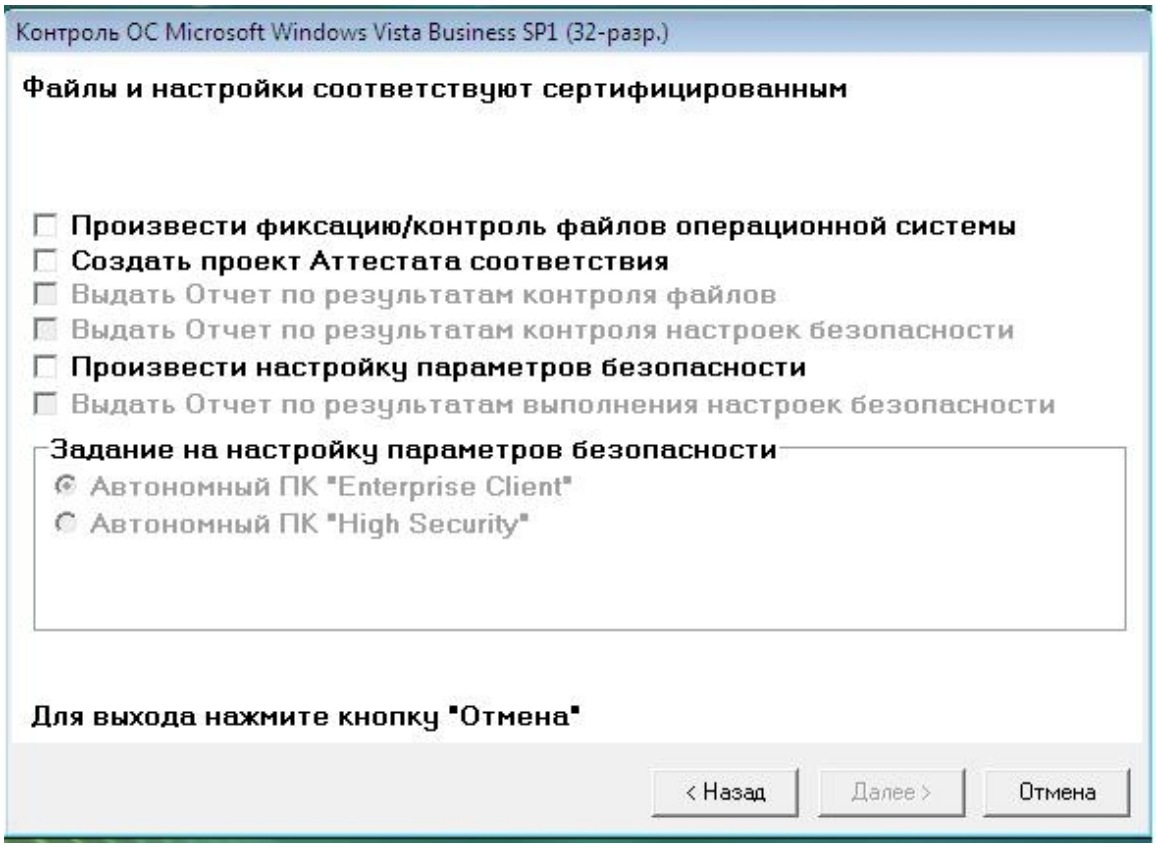

Рисунок 4 – Вид окна программы контроля сертифицированной версии ОС WINDOWS® VISTA™ Service Pack 1 после успешного завершения контроля.

Для создания проекта Аттестата соответствия необходимо щелчком левой кнопки мыши установить флажок «Создать проект Аттестата соответствия» и нажать кнопку «Далее». В появившемся окне, вид которого представлен на рисунке 3, необходимо заполнить предлагаемые поля. Если какое-либо поле останется незаполненным, то в проекте Аттестата в соответствующих местах будет оставлено свободное место для последующего заполнения в текстовом редакторе Microsoft® Word.

Для получения примера заполнения полей окна создания проекта аттестата необходимо нажать кнопку «Пример». Для очистки полей необходимо нажать кнопку «Сброс». Для формирования проекта Аттестата и записи его в файл в формате Microsoft® RTF (Rich Text Format) необходимо нажать кнопку «Далее».

Примечание: если на ПЭВМ не установлен текстовый редактор Microsoft® Word, редактирование и печать файла с проектом Аттестата возможны в редакторе Microsoft® WordPad, входящем в состав ОС WINDOWS® VISTA™ Service Pack 1 .

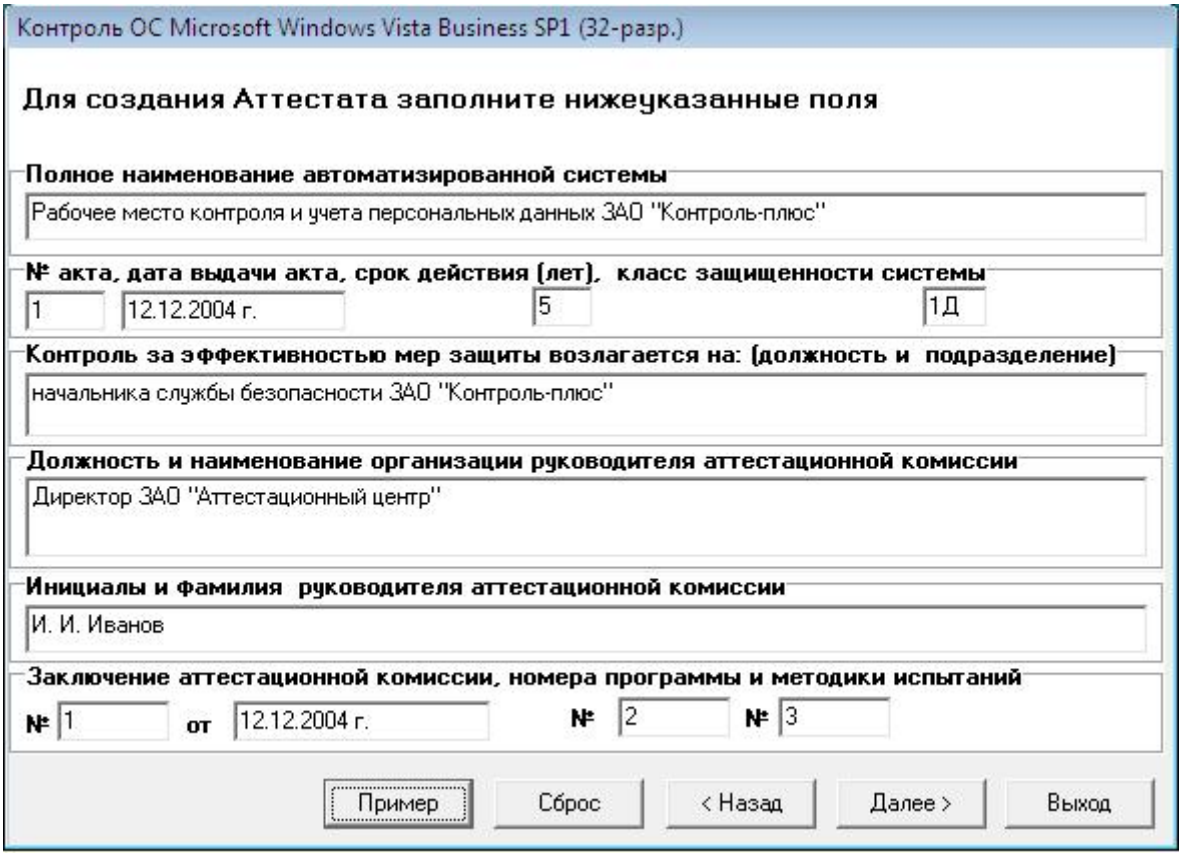

Рисунок 4 – Вид окна программы контроля сертифицированной версии ОС WINDOWS® VISTA™ Service Pack 1 в режиме создания проекта Аттестата соответствия после нажатия кнопки «Пример».

В случае, если соответствие файлов ОС, установленной на ПЭВМ, файлам сертифицированной ОС WINDOWS® VISTA™ Service Pack 1 не установлено, в окне программы, представленном на рисунке 4, будет выведена надпись «Соответствие сертифицированной ОС не установлено», и окно создания проекта Аттестата соответствия не появляется.

При установлении соответствия файлов сертифицированной ОС WINDOWS® VISTA™ Service Pack 1 , но несоответствии настроек параметров безопасности должно появиться окно, представленное на рисунке 5.

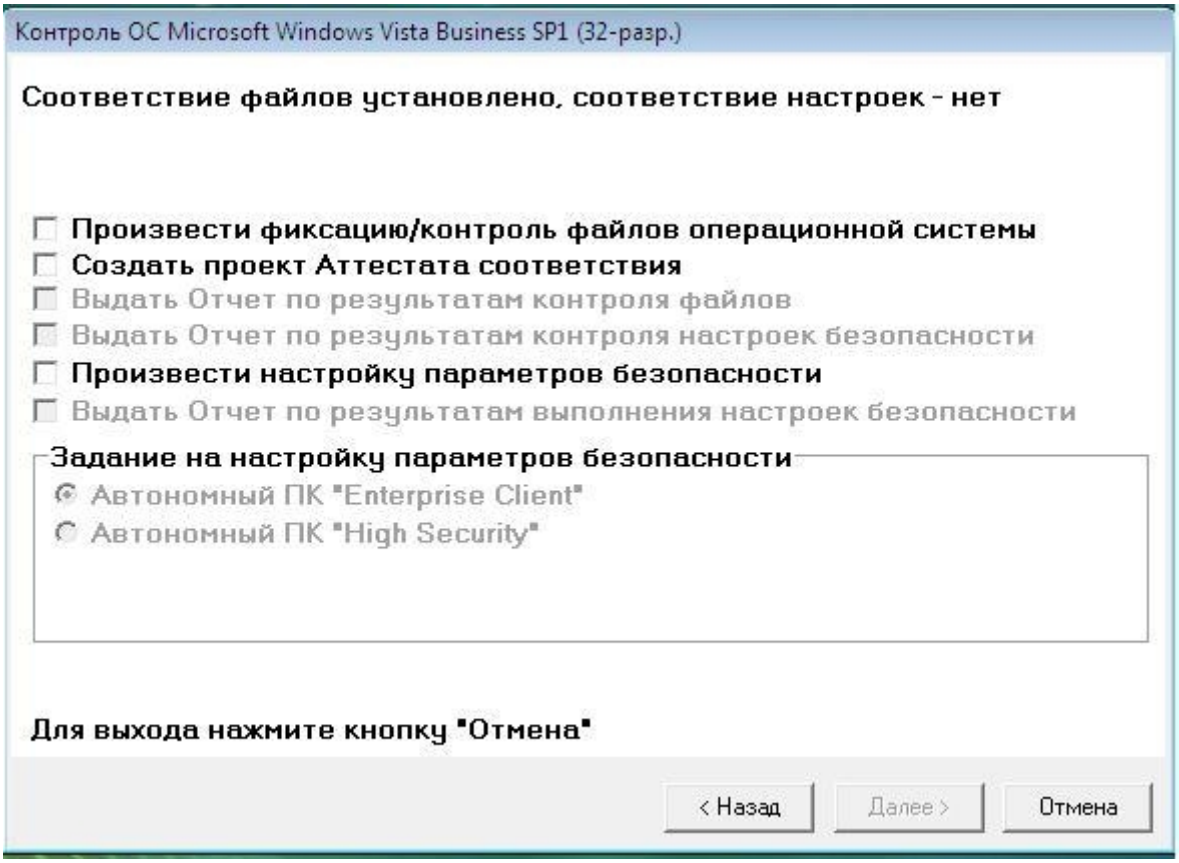

Рисунок 5 – Вид окна программы контроля сертифицированной версии ОС WINDOWS® VISTA™ Service Pack 1 при несоответствии настроек параметров безопасности.

Для создания проекта Аттестата соответствия необходимо установить флажок «Создать проект Аттестата соответствия».

Для создания отчета по результатам контроля настроек безопасности необходимо установить флажок «Выдать отчет по результатам контроля настроек».

При необходимости произвести настройку параметров безопасности следует установить флажок «Произвести настройку параметров безопасности», выбрать один из предложенных шаблонов безопасности - «Автономный ПК Enterprise Client», «Автономный ПК High Security», и нажать кнопку «Далее».

4Комплекс организационно-технических мероприятий по защите конфиденциальной информации на объекте информатизации

4.1 Общие положения

Защита информации на объекте информатизации достигается применением соответствующим образом установленной и настроенной сертифицированной версии операционной системы WINDOWS® VISTA™ Service Pack 1 , выполнением комплекса организационных мероприятий и применением (при необходимости) средств защиты от утечки информации или воздействия на нее по техническим каналам.

При этом основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности информации реализуются без применения сложных технических средств перехвата информации:

- информации, обрабатываемой средствами вычислительной техники, от несанкционированного доступа;
- информации, выводимой на экраны видеомониторов;
- информации, хранящейся на физических носителях.

Разработка мер и обеспечение защиты информации должны осуществляться подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководителями организаций для проведения таких работ.

Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителей организаций, эксплуатирующих объекты информатизации.

Организация работ по защите информации возлагается на руководителей организаций, 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.

Организация работ по созданию и эксплуатации объектов информатизации и их СЗИ должны определяться в «Положении о порядке организации и проведения работ по защите конфиденциальной информации», которое должно содержать:

- 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.

В организации должен быть документально оформлен перечень сведений конфиденциального характера, подлежащих защите в соответствии с нормативными правовыми актами, разработана разрешительная система доступа персонала к такого рода сведениям и определен порядок предоставления пользователям установленных полномочий доступа к соответствующим видам информации, обрабатываемой на объекте информатизации.

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, в организации должен проводиться периодический контроль состояния защиты информации. Контроль осуществляется службой безопасности организации и заключается в оценке:

- соблюдения требований нормативно-методических документов по защите информации;
- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.

4.2Перечень основных мер по защите конфиденциальной информации

На объекте информатизации должен быть реализован ряд организационно-технических мер по защите конфиденциальной информации, основными из которых являются:

- документальное оформление перечня сведений конфиденциального характера;
- ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации, а также к носителям информации на магнитной (магнито-оптической), 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;

- регистрация действий пользователей и обслуживающего персонала при проведении работ на объекте информатизации, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение;
- регулярное дублирование (резервное копирование) массивов и носителей информации;
- размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;
- организация 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;
- предотвращение внедрения программ-вирусов, программных закладок.

В качестве дополнительных организационно-технических мер по защите конфиденциальной информации на объекте информатизации рекомендуются:

- размещение объектов защиты на максимально возможном расстоянии от границы контролируемой зоны;
- использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
- использование дополнительных сертифицированных средств защиты информации;
- использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания);

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.

Носители информации на магнитной (магнито-оптической), оптической и бумажной основе должны учитываться, храниться и уничтожаться в подразделениях организаций в установленном порядке.

В организации, эксплуатирующей объект информатизации, должен быть разработан пакет организационно-распорядительной документации, определяющей:

- 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 учета и хранения носителей информации, содержащих конфиденциальную информацию;
- порядок организации антивирусной защиты;
- порядок организации резервного копирования и восстановления информации;
- ответственность за нарушение установленного порядка работ на объекте информатизации.

При необходимости указанный минимальный набор рекомендуемых организационно-технических мер защиты информации может быть расширен по решению руководителя организации.

Решение о составе и содержании мероприятий, а также используемых средств защиты информации принимается руководителем организации по результатам обследования с учетом важности (ценности) защищаемой информации.

5 ПОЛНЫЙ СПИСОК ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ СЕРТИФИЦИРОВАННОЙ ВЕРСИИ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS® VISTA™ Service Pack 1 (ПРИЛОЖЕНИЕ)

5.1Аппаратная экосистема

- Добавлена поддержка UEFI (Unified Extensible Firmware Interface) - нового промышленного стандарта прошивок (от англ. firmware) для 64-битных систем с функциональной равнозначностью обычным BIOS, что позволит Windows Vista SP1 быть установленным на GPT-диски, а также загружаться и восстанавливаться из режима гибернации с помощью UEFI-прошивок.
- Добавлена поддержка сетевой EFI-загрузки для 64-битных компьютеров.
- Добавлена поддержка 64-битной версии MSDASQL, которая действует в качестве "моста" от OLEDB к различным ODBC-драйверам, что существенно облегчает миграцию приложений с 32-битной платформы на 64-битную Windows Vista.
- Добавлена поддержка Direct3D® 10.1, обновления к Direct3D 10, призванного расширить API для поддержки новых возможностей аппаратного обеспечения, позволяя разработчикам 3D-приложений и игр наиболее эффективно использовать возможности грядущего поколения графических адаптеров.
- Добавлена поддержка exFAT, новой файловой системы, поддерживающей больший объем накопителей и размер файлов, и которая в будущем может быть использована в накопителях на flash-памяти и бытовой технике.
- Добавлена поддержка SD Advanced DMA (ADMA) для совместимых хост-контроллеров SD. Этот новый механизм передачи, который в ближайшее время будет поддерживаться большинством выпускаемых SD-контроллеров, значительно увеличит скорость передачи данных и сократит нагрузку на процессор.
- Добавлена возможность создания DVD-дисков, которые могут быть загружены с помощью BIOS или EFI.

Улучшена поддержка HD-приводов (от англ. high density - высокая емкость), добавлены иконки, идентифицирующие HD-DVD и Blu-ray-приводы в качестве накопителей высокой емкости.

- Добавлена поддержка новых Windows Media Center Extenders, среди которых цифровое телевидение и сетевые DVD-проигрыватели.
- Улучшена поддержка декодирования MPEG-2 с целью обеспечения поддержки защиты контента в системах Media Center, настроенных с помощью цифровых кабельных тюнеров (от англ. digital cable tuner). Данное изменение призвано задействовать высокий уровень

аппаратной акселлерации при воспроизведении коммерческих DVD на некотором типе аппаратного обеспечения.

- Доработано приложение Netproj.exe с целью временно изменить размер экрана для использования различных разрешений при соединении с сетевыми проекторами.

5.2Надежность

Увеличение надежности Windows Vista отличается от компьютера к компьютеру в зависимости от конфигурации компьютера, окружения, а также сценариев использования. Поэтому увеличение надежности у разных пользователей будет разным.

SP1 исправляет большинство самых распространенных сбоев и ошибок Windows Vista, зарегистрированных через Windows Error Reporting. В список исправленных ошибок входят ошибки, связанные с Windows Calendar, Windows Media Player и драйверами, входящими в состав Windows Vista.

Увеличивает надежность работы путем блокировки потери данных на внешних накопителях, отформатированных под файловую систему NTFS.

Увеличивает надежность IPSec-соединений по протоколу IPv6 путем выявления факта, что весь траффик Neighbor Discovery RFC является IPsec-независимым.

Исправляет некоторые сценарии, при которых система отправляет в спящий режим, при этом драйвер не завершил передачу пакетов, путем предоставления драйверу времени, необходимого для завершения передачи пакетов, перед отправкой системы в спящий режим.

Увеличивает надежность беспроводных соединений типа "ad-hoc" (компьютер-компьютер)

Увеличивает успешность пиринговых подключений, как, например, в приложениях Windows Meeting Space или Remote Assistance, когда оба компьютера защищены симметричными брандмауэрами.

Добавляет в инструмент создания резерных копий, встроенный в Windows Vista, возможность добавления в резервную копию файлов, зашифрованных системой EFS.

Включает обновленный инструмент SRT (Startup Repair Tool), являющейся частью среды восстановления Windows (от англ. Windows Recovery environment - WinRE), который теперь может исправлять загрузочные записи жестких дисков даже в случае, если файлы, необходимые для загрузки, повреждены.

Пользователям, отказавшимся принять участие в программе Customer Experience Improvement Program (CEIP), после установки SP1 снова будет предложено принять участие

в программе.

5.3Производительность и электропотребление

Увеличение надежности Windows Vista отличается от компьютера к компьютеру в зависимости от конфигурации компьютера, окружения, а также сценариев использования, поэтому разные пользователи смогут ощутить различный уровень увеличения производительности системы. Порядка 20-25% данных изменений будет реализовано в обновлениях, распространяемых через Windows Update и выпущенных до релиза Windows Vista SP1.

Увеличивает производительность системы и сокращает время отображения сетевых ресурсов.

Сокращает потребление электропитания компьютера в случае, если изображение на экране не меняется в течение определенного времени, что позволяет процессору находится в состоянии пониженного электропитания.

Исправляет проблему с видео-чипсетами (VSync-прерывания), не позволяя системе оставаться в режиме сна.

Сокращает энергопотребление и увеличивает время работы от аккумуляторов засчет исправления проблемы, при котором шпиндель жесткого диска продолжает вращаться даже в случае, если обращений к диску нет.

Увеличивает скорость добавления/извлечения файлов из сжатых (архивированных) папок.

Существенно увеличивает скорость перемещения папок с множеством вложенных файлов.

Увеличивает производительность при копировании файлов с помощью BITS (Background Intelligent Transfer Service).

Увеличивает текущую производительность Windows Vista в следующих сценариях:

1. Быстрее на 25% при копировании файлов в рамках локального компьютера
2. Быстрее на 45% при копировании файлов с компьютера, работающего под управлением системы, отличной от Windows Vista, на компьютер с установленным SP1
3. Быстрее на 50% при копировании файлов с удаленной системы с установленным SP1 на локальный компьютер с установленным SP1

Увеличивает отзывчивость системы при выполнении различных манипуляций с документами или мультимедиа. Например, в оригинальной Windows Vista копирование файлов после удаления других файлов может потребовать гораздо больше времени, чем ожидает пользователь. В SP1 время копирования файлов не зависит от того, были ли до этого удалены какие-либо файлы.

Сокращает время определения ориентировочного времени, необходимого для копирования файлов/папок, при копировании через Windows Explorer до двух секунд.

Сокращает время, необходимое для чтения больших изображений, приблизительно на 50%.

Увеличивает производительность IE при обработке сайтов с Jscript, выводя производительность на уровень предыдущих версий IE.

Исправляет проблему, приводящую к задержке до 5 минут после загрузки системы с определенными типами ReadyDrive-устройств.

Увеличивает эффективность устройств Windows ReadyBoost™, сокращая время, необходимое для восстановления компьютера из режима ожидания/гибернации, за счет увеличения количества информации, хранящейся на ReadyBoost-устройстве.

Включает усовершенствования в Windows Superfetch™, призванные сократить время восстановления компьютера из спящего режима.

В некоторых сценариях SP1 на несколько секунд сокращает время выключения компьютера путем внесения изменений в утилиту, созданную для выполнения синхронизации системы с мобильными устройствами.

Приблизительно на 18% сокращает время выхода из режима ожидания при использовании некоторых типов USB-хабов.

Улучшает некоторые сценарии подключения к сети за счет обновленной логики, которая автоматически выбирает, какой сетевой интерфейс использовать (то есть, какую сеть должен предпочитать ноутбук, если одновременно доступны и проводная сеть и беспроводная).

Увеличивает производительность при авторизации на корпоративных компьютерах вне корпоративной сети, делая ее сравнимой с производительностью компьютера внутри корпоративной сети.

Сокращает время, необходимое для возвращения к работе после использования скринсейвера Photo, делая его сравнимым с временем, необходимым для выхода из режима работы других скринсейверов.

Удаляет задержку, которая иногда имеет место при разблокировании компьютера пользователем.

Увеличивает общую медиа-производительность за счет исправления различного рода ошибок.

После установки SP1 компьютерные администраторы получат возможность смены значения сетевого индекса прерывания для MMCSS (Multimedia Class Scheduling Service), позволяя определять подходящий баланс между сетевой производительностью и качеством воспроизведения аудио/видео.

Windows Vista SP1 включает новый алгоритм сжатия RDP (Remote Desktop Protocol),

который позволит снизить необходимую полосу пропускания сети, необходимую для отправки изображений через RDP. Уровень сжатия, который можно выбрать через настройки групповых политик, прозрачен для всего RDP-траффика и, как правило, позволяет снизить размер RDP-потока примерно на 25-60%.

Инсталлятор Windows Vista SP1 автоматически очищает пользовательские данные, используемые Windows для оптимизации производительности, что может на некоторое время после установки сделать систему менее отзывчивой. По мере использования SP1 система может сохранять подобное состояние в течение нескольких дней, после чего система вновь обретет первоначальную отзывчивость.

SP1 исправляет различные проблемы, связанные с производительностью при использовании новых технологий печати, включая печать XPS.

5.4Безопасность

Windows Vista SP1 включает все ранее выпущенные бюллютени безопасности, предназначенные для Windows Vista.

SP1 включает обновления процесса Secure Development Lifecycle, при котором Microsoft определяла основную причину каждого бюллютеня безопасности и дорабатывала внутренние инструменты, призванные избежать появления ошибок в коде, которые в будущем могут привести к появлению уязвимостей.

Service Pack 1 включает API, благодаря которым сторонние разработчики секьюрити-приложений смогут создавать приложения, которые смогут работать параллельно с технологией Kernel Patch Protection, используемой в 64-битных версиях Windows Vista. Данные API были созданы с целью облегчить секьюрити-вендорам в разработке программного обеспечения, которое сможет расширить возможности ядра Windows в 64-битных системах без отключения защиты Kernel Patch Protection.

Увеличивает безопасность запущенных RemoteApp™-приложений и компьютеров за счет подписи RDP-файлов. Администраторы теперь будут иметь контроль над разграничением прав пользователей в зависимости от цифровых подписей.

Увеличивает безопасность DEP (абб. от Data Execution Protection) за счет добавления новых Win32 API, которые позволяют программный контроль над политика DEP. Это позволит разработчикам приложений контролировать DEP-настройки процесса для обеспечения безопасности, тестируемости, совместимости и надежности.

Увеличивает надежность данных, представленных в Windows Security Center (WSC), за счет выполнения проверки, что только доверенные приложения могут взаимодействовать с WSC.

Увеличивает безопасность проводных сетей за счет включения возможности однократной

аутентификации (от англ. single sign on - SSO) для сетей, требующих аутентификацию. SSO предоставляет пользователю возможность однократного ввода пароля вместо повторного ввода пароля для локальной и сетевой аутентификации.

Для пользователей, обновляющихся с Windows XP до Windows Vista SP1, утилита MSRT (Malicious Software Removal Tool) не может быть запущена. Ежемесячно через Windows Update распространяется обновленная версия MSRT. Доработан криптографический генератор случайных чисел с целью сбора энтропии с множества различных источников, включая Trusted Platform Module (TPM), которые заменяет используемый PRNG на AES-256 для режима пользователя и режима ядра.

Увеличивает безопасность при использовании смарт-карт. Добавляет PIN-канал к ранее собранным PIN-кодам. Данная возможность позволяет избежать множество атак, во избежание которых сегодня требуется использовать внешнее устройство для чтения PIN-кодов. Кроме того, добавляет возможность использования смарт-карт с биометрической аутентификацией вместо аутентификации методом PIN.

Увеличивает безопасность Teredo-интерфейса путем блокировки добровольного траффика. Данное дополнение было реализовано в обновлении безопасности для Windows Vista под номером KB935807.

Усовершенствует BitLocker Drive Encryption путем добавления к методам аутентификации мультифакторной аутентификации, объединяющей ключ, зашитый в TPM (абб. от Trusted Platform Module), со стартовым ключом, хранящимся на USB-драйве, и со сгенерированным пользователем PIN-кодом (абб. от Personal Identification Number).

Добавляет в BitLocker возможность шифрования дисков, отличных от загрузочного диска с Windows Vista (только для Enterprise и Ultimate-редакций).

Усовершенствует реализацию OCSP (абб. от Online Certificate Status Protocol) таким образом, что стало возможным настроить ее для работы с откликами OCSP, подписанными доверенными OCSP-владельцами без необходимости подтверждения сертификата органом, выдавшим сертификат.

Позволяет пользователю со стандартной учетной записью использовать приложение CompletePC Backup. Ранее запустить приложение было позволено лишь администраторам.

Клиент Remote Desktop в Windows Vista SP1 обеспечивает изменения в интерфейсе для клиентской и серверной аутентификации. RDP-клиент сокращает количество шагов, необходимых для подтверждения пользовательских прав к службам Windows Server 2003 (или более ранним) Terminal Server, упрощая управление ранее сохраненными правами.

5.5Новые технологии и стандарты

Добавлена поддержка новых устойчивых алгоритмов шифрования для IPsec: SHA-256, AES-GCM и AES-GMAC для ESP и AH, ECDSA, SHA-256 и SHA-384 для IKE и AuthIP.
К списку доступных в Windows Vista псевдослучайных генераторов чисел (от англ. pseudo-random number generator - PRNG) добавлен NIST SP 800-90 Elliptical Curve Cryptography (ECC).

Добавлена поддержка SSTP (Secure Sockets Tunnel Protocol), удаленного протокола VPN-туннелирования, который войдет в состав платформы Microsoft RRAS (Routing and Remote Access Service). SSTP призван помочь обеспечить VPN-соединения по протоколу SSL, тем самым избавив администраторов от некоторых проблем, связанных с VPN, в частности при использовании NAT, web-прокси-серверов и брандмауэров.

Добавлена поддержка последней версии беспроводного сетевого протокола IEEE 802.11n.

Добавлена поддержка определения идентичности через новые EAPHost API, а также появилась возможность настройки UI для методов туннелирования. Эти API весьма полезны для разработчиков, работающих над методами аутентификации типа "tunneling/multi-phased EAP", а также для тех, кто в своей работе использует EAP-аутентификацию.

Добавлена поддержка Windows Smartcard Framework

Добавлена поддержка Digital Signature Directive и National ID / eID.

Добавлена поддержка ограничений, назначаемых с помощью родительского контроля, через рейтинг Game Rating Board (GRB).

Улучшена поддержка сетевых карт TCP Chimney таким образом, чтобы сетевые карты TCP Chimney смогли обеспечивать поддержку Compound TCP.

Добавлена поддержка беспроводных клиентов для нового режима FIPS (Federal Information Processing). Данный режим является FIPS 140-2-совместимым, потому что благодаря ему процесс шифрования переносится с сетевой беспроводной карты на существующие криптографические FIPS-библиотеки.
Включает обновленный Windows Firewall и IPsec, поддерживающие Suit B-совместимые алгоритмы шифрования.

В состав SP1 не входят драйвера, распространяемые через Windows Update и доступные через сайты производителей компьютеров. Тем не менее, в состав Windows Vista включен набор определенных драйверов (в том числе драйвера для графических карт и звуковых карт) и некоторые из имеющихся в Windows Vista были обновлены.

5.6 Система администрирования и управления

Позволяет пользователям и администраторам выбирать, на каких диска можно выполнять дефрагментацию.

Позволяет пользователям и администраторам использовать инструмент Network Diagnostics для решения большинство проблем, связанных с организацией общего доступа, а не только при проблемах с подключением.

Включает опрос RMS-сервера с регулярными интервалами с целью идентифицировать новые шаблоны и загрузить их в локальное хранилище шаблонов. Ранее эти шаблоны рассылались на клиентские компьютеры при помощи комбинации групповых политик и скриптов. В дополнение к вышесказанному в SP1 добавлен API для приложений, который позволяет опрашивать и получать доступ к шаблонам из локального хранилища.
Windows Vista SP1 включает а новую политику безопасности (UAC: Allow UAccess), которая позволяет приложение требовать подтверждения привилегий пользователя без использования безопасного рабочего стола (от англ. Secure desktop). Это позволит удаленному помощнику подтверждать привилегии администратора в ходе сессии удаленной помощи.

Позволяет администраторам настраивать NAP-клиенты: 1) на прием обновлений с Windows Update или Microsoft Update, в дополнение к WSUS (Windows Server Update Services), используемому в случае с Windows Vista; 2) определить время, в течение которого клиент должен получать и отправлять отчеты о статусе (от англ. Statements of Health). Это позволит NAP-клиентам вовремя отсылать ответы на запросы, когда определенное соединение имеет требование по задержке. Используйте записи DNS-сервера для обнаружения HRA-серверов (абб. от health registration authority), когда отсутствуют настроенные через локальную конфигирацию или групповые политики HRA.

Позволяет работоспособным клиентам, используемым службой поддержки, устанавливать IPSec-подключения к клиентам, на которых есть проблемы, с целью решения проблем. Это увеличивает поддерживаемость NAP, разрешая специалистам службы поддержки устанавливать соединения с любыми компьютерами сети.

Позволяет администраторам добавлять WSD (абб. от Web Services for Devices) Print Device на удаленные компьютеры под управлением Windows Vista или Windows Server 2008. Данное действие может быть осуществлено с помощью консоли управления печатью (от англ. Print Management Console).

Позволяет администраторам исользовать новый флаг, который позволяет использовать WMI-список всего содержимого CSC-кэша. Это существенно упростит администрирование по сценариям WMI для оффлайн-папок в Windows Vista. Ранее это было доступно лишь

через COM API.

Усовершенствует печать на локальных принтерах из сессии Terminal Server. Позволяет пользователям переименовывать или удалять папки при оффлайн-работе с перенаправляемыми папками. Данная функциональность крайне важна для пользователей, пользующихся функцией Folder Redirection и при работе в оффлайн-режиме в течение продолжительного времени. По умолчанию данная возможность отключена, но может быть легко включена путем импорта настроек реестра.

Усовершенствует существующую службу Vista EAPHost путем включения механизма детектирования EAP (абб. от Extensible Authentication Protocol) Certification Program (абб. от ECP). Данный механизм разрешает использование методов EAP, переданных на ECP, которые доступны через Windows Update.

Добавляет WMI-интерфейс в качестве замены инструмента MoveUser.exe, удаленного из состава Windows Vista. Это позволит клиентам проводить переназначение существующей рабочей группы или домена профилей пользователя на новый домен пользовательских профилей.

Позволяет администратору настраивать параметры сети, как, например, имя, и проводить сетевое развертывание с помощью групповых политик.

Разрешает запуск KMS (абб. от Key Management Service) в виртуальной среде (то есть на виртуальной машине).

5.7Установка и развертывание

Значительно упрощает развертывание SP1 в многоязыковой среде, поскольку SP1 содержит 36 языковых пакетов. Однако, это увеличивает размер установочного пакета.

Позволяет пользователям получать обновленные файлы помощи через загружаемые пакеты. Подобный пакет будет выпущен одновременно с SP1.

Добавляет поддержку "горячего патчинга" (от англ. hotpatching), технологии, призванной снизить количество перезагрузок системы. Работает за счет разрешения возможности обновления компонентов Windows в случаях, когда компоненты используются каким-либо из запущенных процессов. Пакеты с поддержкой hotpatching устанавливаются таким же способом, как и традиционные пакеты, и не требуют перезагрузки системы.

Упрощает сценарии миграции и обновления, связанные с компонентами, разрешающими альтернативные способы ввода информации, как речь и перьевой ввод в приложениях, где поддержки этих способов ввода нет.

Упрощает развертывание ОС путем разрешения установки 64-битных версий Windows Vista из 32-битных ОС. Это позволит IT-специалистам проводить обслуживание систем с

помощью всего лишь одного WinPE-образа.

Упрощает развертывание ОС за счет обеспечения поддержки так называемых загрузочных критических драйверов (от англ. offline boot critical storage drivers). WinPE произведет автоматический поиск драйверов на скрытых разделах жестких дисков. Поиск будет осуществлен рекуррентно и при обнаружении этих драйверов они моментально будут загружены. Незагрузочные драйвера (от англ. non-boot critical drivers) будут помечены к загрузке, но не будут загружены до того, как система будет установлена и готова к работе.

Упрощает развертывание патчей путем попыток повторной установки неустановленных обновлений в случаях, когда запрошена установка нескольких обновлений и сбой одного обновления приводит у невозможности установки других.

Увеличивает надежность инсталляции ОС за счет оптимизации инсталлятора таким образом, что он может быть запущен лишь в случае, когда это требуется для установки патча.

Сокращает общее время на установку обновлений путем оптимизации запросов по уже установленным обновлениям.

Увеличивает надежность системы в ходе установки патчей путем обеспечения большей гибкости системы при кратковременных ошибках, как потеря связи с источником.

Увеличивает надежность системы после установки при кратковременных сбоях в ходе очистки файлов ранее установленных ОС.

Упрощает удаление обновлений к ОС путем оптимизации процесса удаления.

Увеличивает надежность установки обновлений путем обеспечения большей гибкости при кратковременных сбоях, как, например, отключение электропитания.

Улучшает инструментарий за счет разрешения отправки дополнительных данных в Microsoft через CEIP (абб. от Customer Experience Improvement Program), когда она включена. Эти данные позволяют идентифицировать множество проблем и сделать ОС более надежной.

После установки SP1-версии OPK (абб. от OEM pre-installation kit) следующие обновления OPK требоваться не будут, в случае если выпущено обновление сервисного стэка (сервисный стэк - это подмножество двочных кодов, используемых для обновления системы). Последующие за SP1 оффлайн-образы могут быть обновлены, используя сервисный стэк, содержащийся в образе, а не в OPK.

5.8Взаимодействие

SP1 позволяет отправку информации Ideal Send Backlog (ISB) на клиенты Winsock2, что обеспечивает более высокую пропускную способность сети при работе с Windows Server 2008. Приложения, оптимизированные для использования нового ISB обеспечат большую

пропускную способность при отправке больших объемов информации на другие компьютеры под управлением Windows Vista или Windows Server 2008. Приложения, которые оптимизации не подвергались, будут работать, как и прежде.
В SP1 внесены изменения в TransmitFile/TransmitPackets и ftp.exe при обмене информацией с Windows Server 2008. Ftp.exe и другие приложения, использующие TransmitFile/TransmitPackets в Windows Vista SP1, получат дополнительную пропускную способность при отправке файлов на другие компьютеры под управлением Windows Vista или Windows Server 2008.

5.9Функции или изменения в API

SP1 удаляет консоль GPMC (Group Policy Management Console), вместо которой для редактирования локальных политик будет использоваться GPEdit. Пользователи SP1 смогут загрузить обновленную версию GPMC, включающую новые возможности редактирования групповых политик, в частности добавление комментариев к объектам групповых политик (или GPO), индивидуальные настройки и поиск по определенным настройкам политик.
В SP1 из Windows Vista Connection Wizard удален MSN Connection Center Dial-up Internet Access .
SP1 включает новый интерфейс Offline Files, предназначенный для нанесения меток "dirty byte" к файлу, измененному в режиме оффлайн. Данный интерфейс работает и через COM API и через WMI provider for Offline Files.

5.10 Общие изменения

В SP1 внесены изменения, которые позволят производителям компьютеров и самим пользователям выбирать поисковый механизм, используемый по умолчанию для поиска по содержимому жесткого диска, по такой же схеме, как сегодня выбирают поисковые механизмы в браузерах и мультимедиа-проигрыватели. Это означает, что в дополнение к множеству способов, которые могут быть использованы для доступа к сторонним поисковым системам в Windows Vista, теперь пользователи смогут осуществлять предпочитаемый ими поиск через дополнительные апплеты в меню Start и Explorer в Windows Vista с установленным SP1. Сторонним разработчикам поисковых приложений для этого потребуется зарегистрировать свои приложения с помощью нового протокола из Windows Vista SP1.
В SP1 сокращено с 4 до 1 количество диалогов UAC (User Account Control), возникающих при создании или переименовании папки в защищенной области ОС.
Изменения в интерфейсе и поведении системы, призванные помочь пользователю при

активации: более подробные подсказки, коды ошибок заменены на описания.

В SP1 внесены изменения в текст в панели Ultimate Extras Control Panel с целью описания программы Ultimate Extras в более общих терминах.

Изменено поведение при сканировании изображений через встроенные средства Vista SP1: после сканирования будет открыто окно Explorer, а не Windows Photo Gallery, как это было ранее.

В ходе установки Windows Vista SP1 пользователи обязаны вводить подсказку к паролю. Данное изменение было внесено на базе отзывов от производителей компьютеров, утверждающих, что пользователи часто забывают пароли, а поскольку учетная запись администратора в Windows Vista по умолчанию отключена, пользователи никак не могут получить доступ к своим компьютерам. Подсказка к паролю призвана предотвратить подобные сценарии.

Увеличена совместимость со сторонними диагностическими утилитами, работа которых основана на Raw Socket, путем использования той же самой логики для управления (ICMP v4 и v6) и систематизации пакетов.

Несмотря на то, что в данной сборке это не реализовано, в финальной версии SP1 будут реализованы изменения, которые позволят разграничить возможности пользователей лицензионных и нелицензионных версий ОС. Подобные изменения будут внесены на базе отзывов от VL-клиентов.

Также в состав будущих сборок SP1 будут включены обновления, блокирующие два эксплойта, которые мргут негативно сказываться на стабильности работы: 1) эксплойт типа OEM Bios, подразумевающий модификацию системных файлов и BIOS материнской платы таким образом, чтобы имитировать активацию тех копий Windows, которые устанавливаются OEM-производителями на заводах по сборке; эксплойт типа Grace Timer, который увеличивает "пробный период" между установкой ОС и активацией в некоторых случаях до 2099 года.

5.11 Соответствие между Windows Vista и Windows Server 2008

Между Windows Vista и Windows Server 2008 установлено соответствие, то есть большинство файлов обоих продуктов идентичны. В результате такого дизайна имеют место такие случаи, когда код изменен таким образом, чтобы активировать серверный сценарий, который не имеет влияния или ограниченно имеет влияние на возможности Windows Vista SP1. Вот несколько примеров:

Общий доступ: Подсистема общего доступа в Windows Vista разрешает всего лишь 10 входящих соединений одновременно. Windows Server 2008 же должен разрешать тысячи

входящих соединений. В ходе тестирования и приема отзывов в ходе разработки Windows Server 2008, подсистема общего доступа была настроена и оптимизирована так, чтобы стэк общего доступа стал более производительным, надежным и масштабируемым. Подобный уровень настройки неприменим к клиентским машинам, допускающим лишь 10 соединений одновременно, но критичен для роли файл-сервера. Подобные изменения предназначены, как правило, для серверных сценариев, хотя от них выиграет и Windows Vista SP1.

IIS 7: IIS включен в некоторые версии Windows Vista с целью помочь web-разработчикам создавать и тестировать свои приложения. IIS в Windows Server 2008 является важной серверных ролью, которая требует масштабируемости уровня "Интернет" и высокой производительности. С момента релиза Windows Vista компоненты IIS7 подверглись серьезной доработке в плане производительности и надежности, чтобы отвечать требованиям высоко-масштабируемого серверного компонента. Данные изменения не затронут большинство пользователей Windows Vista, у которых компоненты IIS7 не установлены. Тем не менее, поскольку между Windows Vista и Windows Server проведено соответствие, эти изменения включены в состав Windows Vista SP1.

Подключение нескольких пользователей: В Windows Vista для возможности переключения между различными пользователями требуются две ключевые подсистемы: Windows Logon process и Core kernel. Однако, в Windows Server 2008, куда включен Terminal Server, могут существовать тысячи одновременно подключенных пользователей, данные системы должны быть настроены на максимальную производительность и надежность. Подобные изменения предназначены, как правило, для серверных сценариев, хотя от них выиграет и Windows Vista SP1.