Код безопасности
ГК «Информзащита»

Средство защиты информации

SECRET NET 6

Руководство администратора

Управление. Полномочное управление доступом и контроль печати

RU.88338853.501410.007 91 4

Почтовый адрес:	**127018, г. Москва, ул. Сущёвский Вал, дом 47, стр. 2, помещение №1**
Телефон:	**(495) 980-23-45**
Факс:	**(495) 980-23-45**
e-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Версия: 6.5 Последнее обновление: 14-09-10

Оглавление

Список сокращений

FAT	File Allocation Table
LFN	Long File Name
NTFS	New Technology File System
MS	Microsoft
RTF	Reach Text Format
ОС	Операционная система
ПО	Программное обеспечение

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net 6" RU.88338853.501410.007 (далее — система Secret Net 6, система защиты). В руководстве содержатся сведения, необходимые администраторам для настройки механизма полномочного разграничения доступа (называемого также "механизм полномочного управления доступом").

Перед изучением руководства необходимо ознакомиться с документами [1], [3].

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru и hotline@infosec.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем учебного центра можно по электронной почте (edu@infosec.ru).

Глава 1
Общие сведения

Механизм полномочного управления доступом обеспечивает разграничение доступа пользователей к конфиденциальным ресурсам (каталогам, файлам), находящимся на дисках с файловой системой NTFS. Разграничение осуществляется на основе сопоставления уровня допуска пользователя и категории конфиденциальности ресурса. Для работы с конфиденциальными файлами могут использоваться любые приложения.

Полномочное управление доступом не отменяет действие других средств управления доступом. Например, если пользователю не предоставлен доступ к файлу средствами ОС Windows, то даже при наличии нужных прав доступа к конфиденциальной информации пользователь не сможет осуществить доступ к этому файлу.

Категории конфиденциальности и уровни допуска

Категории конфиденциальности ресурсов

В механизме полномочного управления доступом используются следующие категории конфиденциальности:

- "неконфиденциально";
- "конфиденциально";
- "строго конфиденциально".

Категория конфиденциальности относится к атрибутам ресурса (каталога или файла). Названия категорий, предлагаемые по умолчанию, можно изменить.

После установки клиентского ПО системы Secret Net 6 всем ресурсам компьютера, не имевшим ранее присвоенных категорий конфиденциальности, назначается категория "неконфиденциально". Повышение категорий конфиденциальности нужных файлов осуществляется пользователями в пределах своих уровней допуска. При этом понижать категории конфиденциальности ресурсов, а также повышать категории каталогов разрешено только пользователям, которым предоставлена привилегия на управление категориями конфиденциальности.

Наследование категории конфиденциальности

В механизме полномочного управления доступом используется принцип наследования файлами категории конфиденциальности каталога. Принцип наследования действует для каталогов, имеющих категорию "конфиденциально" или "строго конфиденциально".

Признак наследования категории конфиденциальности относится к атрибутам каталога. Установка признака выполняется пользователем при условии наличия у него привилегии на управление категориями конфиденциальности.

Присвоение новым файлам категории конфиденциальности каталога может выполняться автоматически или по запросу. Включение и отключение режима автоматического присвоения категории осуществляется в диалоговом окне настройки свойств каталога (параметр "Автоматически присваивать новым файлам").

Уровни допуска пользователей

Доступ пользователя к информации, содержащейся в конфиденциальном файле, осуществляется при условии, если пользователю назначен соответствующий уровень допуска. Набор уровней допуска, применяемых в системе, совпадает с набором категорий конфиденциальности ресурсов (см. выше).

Пользователю разрешается доступ к файлу, если уровень допуска пользователя не ниже категории конфиденциальности файла. Например, пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями "конфиденциально" и "неконфиденциально", но запрещено открывать файлы с категорией "строго конфиденциально". Уровень допуска

"строго конфиденциально" предоставляет возможность открывать файлы с любой категорией конфиденциальности.

По умолчанию всем пользователям назначен уровень допуска "неконфиденциально". Описание процедуры назначения уровня допуска см. на стр. 11.

Привилегии пользователей

В механизме полномочного управления доступом могут действовать привилегии, перечисленные в следующей таблице:

Привилегия	Описание
Управление категориями конфиденциальности	Пользователь может: • изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска; • управлять режимом наследования категорий конфиденциальности каталогов (см. стр. 12).
Печать конфиденциальных документов	Используется для разрешения пользователю выводить на принтер конфиденциальные документы. Привилегия применяется при включенном режиме контроля печати конфиденциальных документов
Вывод конфиденциальной информации	Пользователю разрешается выводить конфиденциальную информацию на внешние носители при включенном режиме контроля потоков

Привилегии предоставляются администратором безопасности пользователям, уполномоченным управлять конфиденциальностью ресурсов, распечатывать и копировать конфиденциальную информацию (см. стр. 11). По умолчанию пользователям привилегии не предоставлены.

Режимы работы механизма полномочного управления доступом

Контроль потоков

Режим контроля потоков обеспечивает предотвращение несанкционированного распространения конфиденциальной информации. Под распространением понимается вывод конфиденциальной информации на внешние носители (сменные диски, флэш-накопители и т. п., а также жесткие диски с файловой системой, отличной от NTFS), которые могут быть извлечены из системы или на которых конфиденциальные файлы теряют признак конфиденциальности. Кроме того, в режиме контроля потоков блокируется несанкционированное понижение категории конфиденциальности ресурса (файла или каталога).

При включенном режиме контроля потоков возможность доступа пользователя к конфиденциальным файлам определяется уровнем конфиденциальности сессии, который устанавливается при входе пользователя в систему (см. ниже). При этом осуществляется контроль вывода конфиденциальной информации на внешние носители.

Если контроль потоков отключен, система не контролирует распространение конфиденциальной информации. При попытке доступа к конфиденциальному файлу проверяется уровень допуска пользователя и категория конфиденциальности ресурса.

По умолчанию режим контроля потоков отключен.

Уровень конфиденциальности сессии

Если включен режим контроля потоков, пользователи для работы на компьютере должны открывать сессии с определенным уровнем конфиденциальности. Уровень сессии выбирается пользователем при входе в систему. Уровень сессии не может быть выше уровня допуска, назначенного пользователю.

После открытия сессии при выполнении пользователем операций с конфиденциальными ресурсами категории конфиденциальности ресурсов сравниваются с уровнем сессии. Выполнение операции разрешено, если категория конфиденциальности ресурса ниже или совпадает с уровнем сессии. При этом после выполнения операции копирования или сохранения файла его категория

автоматически повышается (при необходимости) до текущего уровня конфиденциальности сессии.

В зависимости от типа входа в систему уровень конфиденциальности сессии выбирается самим пользователем или автоматически назначается системой. Если осуществляется вход локального или доменного пользователя с использованием стандартного интерактивного диалога приветствия, пользователь сам выбирает уровень конфиденциальности сессии. Если осуществляется сетевой вход или вход без использования стандартного интерактивного диалога приветствия (например, при запуске приложения от имени другого пользователя), сессии автоматически назначается самый низший уровень конфиденциальности.

Таким образом, выбирая уровень конфиденциальности сессии, пользователь тем самым определяет категорию конфиденциальности для документов, с которыми предполагает работать. Так, например, с уровнем допуска "строго конфиденциально" пользователь может выбрать уровень конфиденциальности сессии "конфиденциально" и тем самым запретить доступ к строго конфиденциальным документам. Однако следует иметь в виду, что неконфиденциальные документы, с которыми выполняются операции копирования и сохранения в конфиденциальной сессии, после выполнения операции станут конфиденциальными.

Уровень конфиденциальности сессии нельзя изменить на протяжении всего сеанса работы пользователя.

Контроль печати конфиденциальных документов

Режим контроля печати конфиденциальных документов обеспечивает предотвращение несанкционированного вывода на печать документов, имеющих категорию "конфиденциально" или "строго конфиденциально".

Если контроль печати конфиденциальных документов отключен, любому пользователю, который имеет доступ к конфиденциальному файлу, разрешено распечатывать этот файл. При печати в документ не добавляется гриф конфиденциальности.

При включенном режиме контроля печати конфиденциальных документов для пользователей действуют следующие ограничения:

- распечатывать конфиденциальные документы разрешено только пользователям, которым предоставлена привилегия "Печать конфиденциальных документов". Если данная привилегия пользователю не предоставлена, он может печатать только неконфиденциальные документы;
- при печати конфиденциальных документов в обязательном порядке добавляется гриф конфиденциальности.

Факт печати конфиденциального документа регистрируется в журнале.

По умолчанию режим контроля печати конфиденциальных документов отключен.

Глава 2
Правила работы с конфиденциальными ресурсами

В данном разделе приведены обобщенные правила работы с конфиденциальными документами в условиях работающего механизма полномочного управления доступом. Ниже в таблице приведены правила работы, действующие при отключенном и включенном режиме контроля потоков конфиденциальной информации.

<table>
<tr><th>Без контроля потоков</th><th>При контроле потоков</th></tr>
<tr><th colspan="2">Доступ к файлам</th></tr>
<tr><td>Доступ пользователя к файлу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности файла</td><td>Доступ пользователя к файлу разрешается, если уровень конфиденциальности пользовательской сессии не ниже категории конфиденциальности файла</td></tr>
<tr><td>Запрещено удаление конфиденциального файла с помещением в "Корзину"</td><td>Запрещено удаление любого файла с помещением в "Корзину"</td></tr>
<tr><th colspan="2">Доступ к каталогам</th></tr>
<tr><td colspan="2">Конфиденциальные файлы размещаются в каталогах, имеющих категорию конфиденциальности не ниже категории конфиденциальности файла. Например, в каталоге с категорией "конфиденциально" могут размещаться как неконфиденциальные файлы, так и файлы с категорией "конфиденциально"</td></tr>
<tr><td colspan="2">Пользователь, не имеющий доступ к файлу, может просмотреть содержимое конфиденциального каталога, в котором находится файл, но не может открыть файл. Поэтому названия конфиденциальных файлов не должны содержать конфиденциальную информацию</td></tr>
<tr><td>Запрещено удаление конфиденциального каталога с помещением в "Корзину"</td><td>Запрещено удаление любого каталога с помещением в "Корзину"</td></tr>
<tr><th colspan="2">Наследование категории конфиденциальности каталога</th></tr>
<tr><td>Если включен режим автоматического присвоения категории конфиденциальности, при создании, сохранении, копировании или перемещении файла в каталог файлу присваивается категория конфиденциальности каталога</td><td>Если включен режим автоматического присвоения категории конфиденциальности, при создании, сохранении, копировании или перемещении файла в каталог файлу присваивается категория конфиденциальности каталога. Ограничение: устанавливаемая категория конфиденциальности должна быть равна текущему уровню конфиденциальности сессии</td></tr>
<tr><td>Если отключен режим автоматического присвоения категории конфиденциальности:
при создании, сохранении или копировании файлу присваивается категория "неконфиденциально";
при перемещении файла внутри логического раздела файл сохраняет свою категорию конфиденциальности (при этом перемещение файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности каталога).</td><td>Если отключен режим автоматического присвоения категории конфиденциальности:
при создании, сохранении или копировании файлу присваивается категория, соответствующая уровню конфиденциальности сессии, но не выше категории конфиденциальности каталога;
при перемещении файла внутри логического раздела файл сохраняет свою категорию конфиденциальности (при этом перемещение файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности каталога и уровень конфиденциальности сессии).</td></tr>
<tr><td colspan="2">Каталоги с отключенным режимом автоматического присвоения категории конфиденциальности целесообразно использовать для хранения файлов с различными категориями конфиденциальности (меньшими или равными категории конфиденциальности каталога). Чтобы исключить неожиданное изменение категорий конфиденциальности файлов после выполнения операций с ними, рекомендуется использовать каталоги, для которых установлено одинаковое состояние режима автоматического присвоения категории</td></tr>
</table>

Без контроля потоков	При контроле потоков
Работа в приложениях	
Приложению присваивается уровень конфиденциальности, равный наивысшей категории конфиденциальности среди открытых в приложении файлов. Уровень конфиденциальности приложения не снижается после закрытия конфиденциального файла и сохраняется до закрытия приложения. Чтобы сохранить файл с более низкой категорией конфиденциальности, чем текущий уровень приложения, необходимо закрыть приложение и открыть его заново	Приложению присваивается уровень конфиденциальности, равный текущему уровню сессии пользователя. Разрешается открывать файлы не выше этого уровня. Категория файлов с более низким уровнем конфиденциальности повышается до уровня конфиденциальности сессии (повышение категории происходит при сохранении файла)
Некоторые приложения при запуске автоматически обращаются к определенным файлам — например, к ранее открывавшимся файлам в приложении. При этом не происходит непосредственное открытие файла (документа). В силу особенностей механизма полномочного управления доступом, при таких обращениях к конфиденциальным и строго конфиденциальным файлам пользователю предлагается повысить уровень конфиденциальности приложения до уровня конфиденциальности этих файлов. В таких случаях, если не планируется работать с предложенным уровнем конфиденциальности, достаточно отказаться от повышения уровня конфиденциальности приложения	
Изменение категории конфиденциальности ресурса	
Пользователь, **не** обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше своего уровня допуска (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога)	Пользователь, **не** обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше уровня конфиденциальности сессии (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога)
Пользователь, обладающий привилегией "Управление категориями конфиденциальности", может: • повысить категорию конфиденциальности каталогов и файлов, но не выше уровня допуска пользователя; • понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше уровня допуска пользователя; • изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше уровня допуска пользователя.	Пользователь, обладающий привилегией "Управление категориями конфиденциальности", может: • повысить категорию конфиденциальности каталогов и файлов, но не выше текущего уровня сессии; • понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше текущего уровня сессии; • изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше текущего уровня сессии.
Печать конфиденциальных документов	
Если включен режим контроля печати: • пользователь, **не** обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы; • пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей уровень допуска пользователя.	Если включен режим контроля печати: • пользователь, **не** обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы (если документ не редактировался); • пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей текущий уровень сессии.
Если отключен режим контроля печати конфиденциальных документов, любому пользователю, имеющему доступ к конфиденциальным документам, разрешен вывод этих документов на печать независимо от наличия у него привилегии "Печать конфиденциальных документов". При этом документы распечатываются без грифа конфиденциальности	
При включенном режиме контроля печати для печати конфиденциальных документов можно использовать только приложения MS Word или MS Excel. Печать из других приложений блокируется. При печати в документы автоматически добавляется выбранный гриф конфиденциальности	

Без контроля потоков	При контроле потоков
Вывод на внешние носители	
Пользователь, имеющий доступ к конфиденциальным документам, может копировать файлы или сохранять их содержимое на любые носители независимо от наличия привилегии "Вывод конфиденциальной информации"	Пользователь, **не** обладающий привилегией "Вывод конфиденциальной информации", не может копировать конфиденциальные файлы или сохранять их содержимое на внешние носители. Внешними носителями считаются: • **в базовом режиме контроля вывода информации** (включен по умолчанию) — любые встроенные и съемные носители информации с файловой системой, отличной от NTFS (например, жесткий диск или дискета с FAT); • **в расширенном режиме контроля вывода информации** — любые встроенные носители информации с файловой системой, отличной от NTFS (например, жесткий диск с FAT), а также любые съемные носители информации (например, дискета с NTFS или FAT).

Глава 3
Настройка механизма

Общий порядок настройки

Для использования на компьютерах механизма полномочного управления доступом выполните настройку в следующем порядке:

1. Назначьте пользователям уровни допуска и привилегии (см. ниже).
2. Присвойте ресурсам категории конфиденциальности (см. стр. 12).
3. Настройте перечень регистрируемых событий (см. стр. 12).
4. При необходимости включите режим контроля потоков (см. стр. 12).
5. При необходимости включите режим контроля печати (см. стр. 13).
6. При необходимости измените названия категорий (см. стр. 13).
7. При необходимости настройте грифы конфиденциальности (см. Главу **4**).

В документе с комментариями к выпущенной версии (Release Notes) приведены последние рекомендации разработчиков по настройке механизма для работы с приложениями.

Перед вводом механизма в использование разъясните пользователям правила работы с конфиденциальными ресурсами.

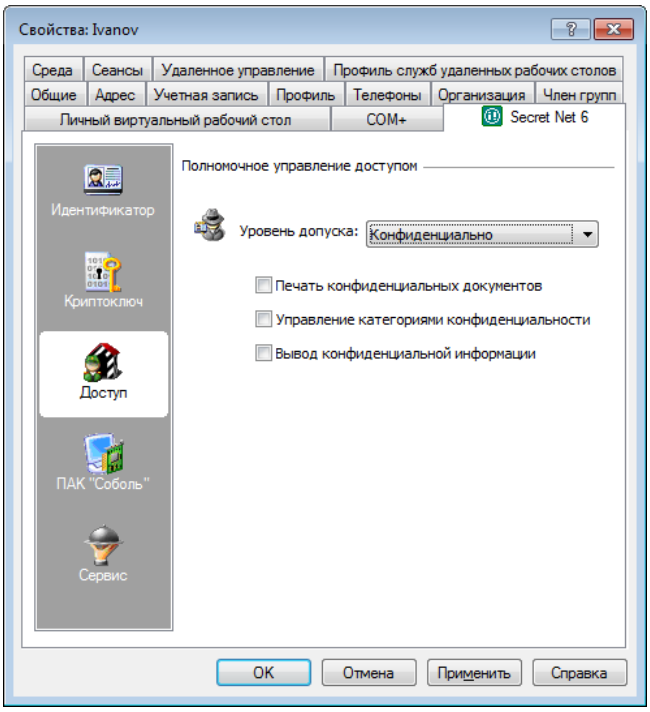
Назначение уровней допуска и привилегий пользователям

Уровень допуска и привилегии назначаются администратором безопасности каждому пользователю индивидуально.

Привилегия может быть назначена пользователю при условии, если ему назначен уровень допуска к конфиденциальной информации.

Для назначения уровня допуска и привилегий:

1. Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 6" (описание процедуры вызова оснастки см. в документе [3]).
2. В панели выбора режима выберите режим "Доступ".



3. Установите уровень допуска пользователя в одноименном поле.

   Для уровней "конфиденциально" и "строго конфиденциально" становится доступным назначение привилегий.

4. Для предоставления или отмены привилегий пользователя установите или удалите отметки в соответствующих полях.

5. Нажмите кнопку "OK".

Параметры вступят в силу при следующем входе пользователя в систему.

Присвоение категорий конфиденциальности ресурсам

Присвоение ресурсам категорий конфиденциальности выполняется уполномоченными пользователями, имеющими привилегию "Управление категориями конфиденциальности". Категория конфиденциальности может быть присвоена только ресурсам, расположенным на дисках с файловой системой NTFS.

Описание процедур изменения категории конфиденциальности каталогов и файлов см. в документе [9].

Внимание! При присвоении ресурсам категорий конфиденциальности учитывайте следующие общие рекомендации:

- Не присваивайте категории "конфиденциально" и "строго конфиденциально" системным каталогам, каталогам, в которых размещается прикладное программное обеспечение, а также каталогу "Мои документы" и всем подобным ему.
- Во избежание непроизвольного повышения категорий конфиденциальности файлов храните файлы в каталогах с категорией конфиденциальности, равной категории конфиденциальности файлов.

Настройка регистрации событий

Для отслеживания произошедших событий, связанных с работой механизма полномочного управления доступом, необходимо выполнить настройку регистрации событий. Для этого следует указать, какие события категорий "Полномочное управление доступом" и "Контроль печати" должны регистрироваться в журнале Secret Net. Полный перечень событий этих категорий и процедура настройки регистрации событий приведены в документе [5].

По умолчанию после установки клиентского ПО системы защиты в локальной политике безопасности компьютера включена регистрация всех событий, связанных с работой механизма полномочного управления доступом и контроля печати.

Управление режимом контроля потоков

По умолчанию режим контроля потоков конфиденциальной информации отключен.

Для включения или отключения режима контроля потоков:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (описание процедуры вызова оснастки см. в документе [3]).

2. Выберите папку "Настройки подсистем".

   В правой части окна появится список параметров.

3. Вызовите контекстное меню для параметра "Полномочное управление доступом: Режим работы" и активируйте в нем команду "Свойства".

   На экране появится диалог настройки параметра.

4. Включите или отключите действие режима, установив отметки в соответствующих полях.

5. Для включения контроля потоков в расширенном режиме установите отметку в поле "Расширенный контроль вывода информации".

6. Нажмите кнопку "OK".

Управление режимом контроля печати конфиденциальных документов

По умолчанию режим контроля печати конфиденциальных документов отключен.

Для включения или отключения режима контроля печати:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (описание процедуры вызова оснастки см. в документе [3]).
2. Выберите папку "Настройки подсистем".

   В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Полномочное управление доступом: Режим контроля печати конфиденциальных документов" и активируйте в нем команду "Свойства".

   На экране появится диалог настройки параметра.
4. Включите или отключите действие режима, установив отметки в соответствующих полях, и нажмите кнопку "ОК".

Изменение названий категорий конфиденциальности

Используемые по умолчанию названия категорий и уровней конфиденциальности ("неконфиденциально", "конфиденциально" и "строго конфиденциально") можно заменить другими названиями, принятыми в организации.

Для ввода названий категорий конфиденциальности:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (описание процедуры вызова оснастки см. в документе [3]).
2. Выберите папку "Настройки подсистем".

   В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Полномочное управление доступом: Названия уровней конфиденциальности" и активируйте в нем команду "Свойства".

   На экране появится диалог настройки параметра.
4. В соответствующих полях введите названия категорий и нажмите кнопку "ОК".

   Для восстановления используемых по умолчанию названий нажмите кнопку "Вернуть исходные".

Глава 4
Управление грифами конфиденциальности

В режиме контроля печати конфиденциальных документов для маркировки документов, выводимых на печать в приложениях MS Word и MS Excel, используются грифы конфиденциальности. По умолчанию в системе сформировано по два грифа (Гриф#1 и Гриф#2) для каждого из указанных приложений.

Гриф представляет собой набор полей, которые заполняются сведениями о документе. Поля заполняются автоматически приложением или пользователем по запросу системы. Содержимое грифа может быть представлено в колонтитулах и на последней странице распечатанного документа.

При печати документов пользователи выбирают нужный гриф из числа имеющихся в системе. Оформление грифа и набор полей определяется в шаблоне, который может редактироваться администратором безопасности.

В сетевом режиме функционирования системы Secret Net 6 шаблон грифов конфиденциальности может быть задан как локально, так и централизованно. По умолчанию шаблоны грифов заданы в локальной политике безопасности компьютеров, на которых установлено клиентское ПО системы Secret Net 6. Если шаблон задан централизованно, на компьютерах с установленным клиентским ПО в сетевом режиме функционирования будут применяться грифы, хранящиеся в Active Directory.

Описание грифов по умолчанию и порядок действий для выбора грифа при печати конфиденциальных документов см. в документе [9].

Редактирование шаблона грифов для MS Word

Шаблон грифов конфиденциальности для MS Word реализован в виде RTF-файла. Внутри файла грифы отделены друг от друга разрывами разделов (в терминологии MS Word). В шаблоне можно отредактировать имеющиеся встроенные грифы и добавить произвольное количество других грифов.

Для редактирования RTF-файла шаблона на компьютере должен быть установлен редактор MS Word.

Ввод в действие шаблона и загрузка для редактирования

Ввод в действие шаблона и его загрузка для редактирования осуществляется в оснастке для управления параметрами объектов групповой политики.

Для ввода в действие отредактированного шаблона:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (описание процедуры вызова оснастки см. в документе [3]).
2. Выберите папку "Настройки подсистем".

   В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Полномочное управление доступом: Гриф конфиденциальности для Microsoft Word" и активируйте в нем команду "Свойства".

   На экране появится диалог настройки параметра.
4. Нажмите кнопку "Редактировать".

   На экране появится окно редактора MS Word с загруженным файлом шаблона.
5. Отредактируйте файл шаблона (см. ниже), сохраните и закройте окно редактора.
6. Нажмите кнопку "OK".

Для ввода в действие шаблона по умолчанию:

1. Выполните действия **1**–**3** вышеописанной процедуры.
2. Нажмите кнопку "Вернуть исходный".

3. Нажмите кнопку "OK".

   Ранее заданный шаблон будет удален, и в систему будет загружен встроенный шаблон (используемый по умолчанию после установки системы Secret Net 6).

Формирование списка грифов

Добавление нового грифа в шаблон

Добавление грифа заключается во вставке в шаблон нового раздела с необходимым набором полей. Как правило, при добавлении грифа целесообразно взять за основу имеющиеся грифы шаблона. Если для редактирования предполагается использовать имеющийся колонтитул, новый раздел следует вставить после раздела, содержащего этот колонтитул. В этом случае в новый раздел будут скопированы колонтитулы предыдущего раздела.

Если добавляемый гриф в значительной степени отличается от имеющихся и для него не требуется копировать и редактировать колонтитулы, новый раздел можно вставить в конце любого раздела. Рекомендуется вставить его в конце последнего раздела файла шаблона.

Для добавления грифа:

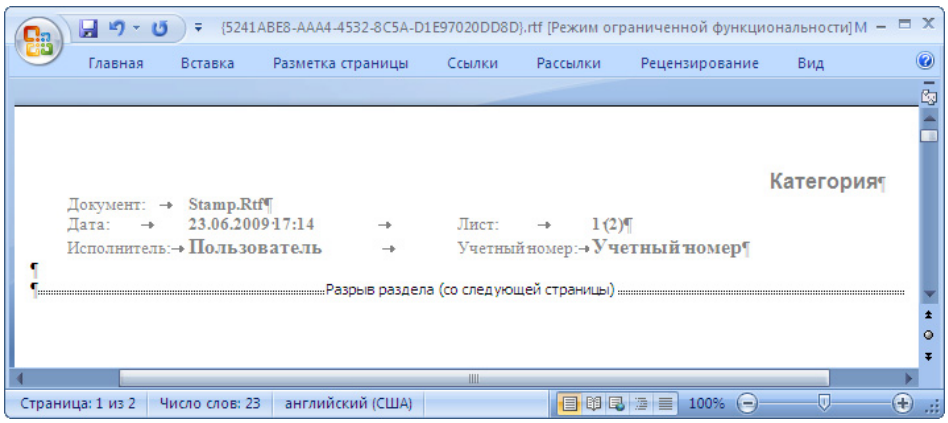
1. Вызовите файл шаблона для редактирования (см. выше).

Совет. Для удобной работы с шаблоном рекомендуется включить режим отображения всех знаков форматирования в редакторе MS Word. Включение режима осуществляется с помощью кнопки "Непечатаемые знаки". В зависимости от версии установленной программы MS Word эта кнопка размещается:

- в MS Word 2007 — на вкладке "Главная" в группе "Абзац";
- в MS Word 2003 и более ранних версиях — на панели инструментов "Стандартная".

2. Установите курсор в начало строки разрыва раздела и нажмите клавишу <Enter>.

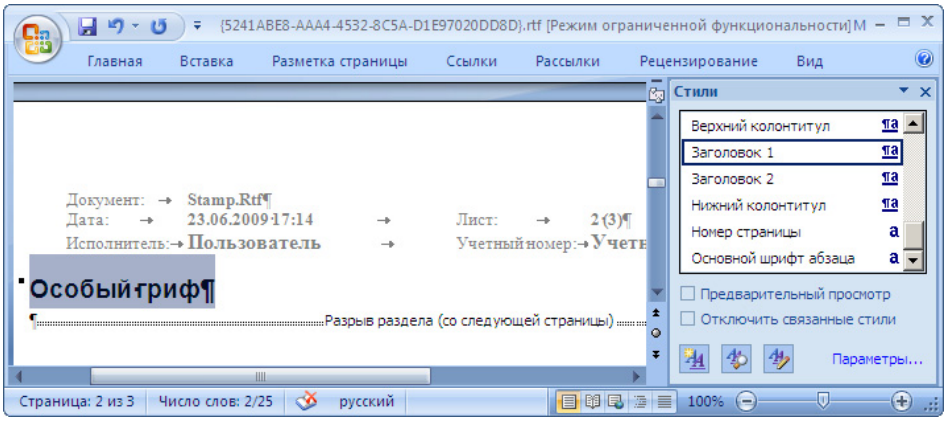
   Перед разрывом раздела будет вставлен пустой абзац:



3. Установите курсор в пустой абзац перед разрывом раздела и вставьте новый раздел. Для этого в зависимости от версии установленной программы MS Word выполните соответствующее действие:
   - в MS Word 2007 — перейдите на вкладку "Разметка страницы" и в группе "Параметры страницы" активируйте команду "Разрывы | Следующая страница";
   - в MS Word 2003 и более ранних версиях — в меню "Вставка" активируйте команду "Разрыв...", в появившемся диалоге отметьте поле "Новый раздел: со следующей страницы" и нажмите кнопку "OK".

   В документ будет вставлен новый раздел с колонтитулами, скопированными из предыдущего грифа.
4. Отредактируйте содержимое колонтитулов.

5. В первом пустом абзаце после верхнего колонтитула введите название грифа, отформатированное стилем "Заголовок 1":



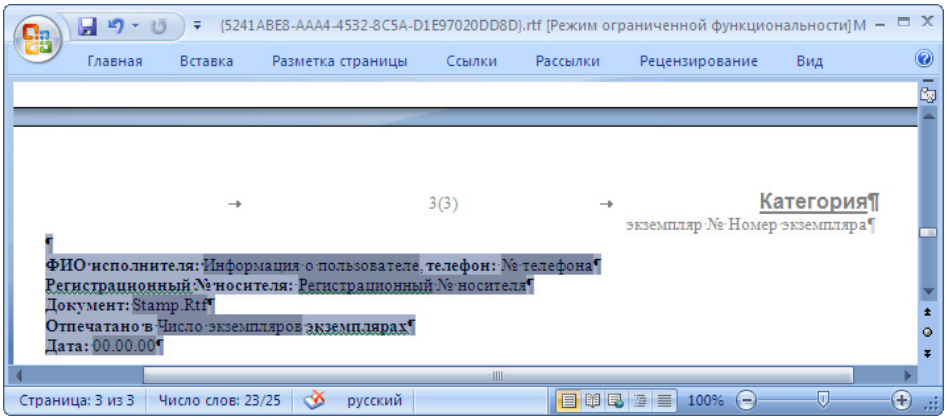
6. При необходимости добавьте после названия грифа абзацы, содержащие нужные поля.

Удаление грифа

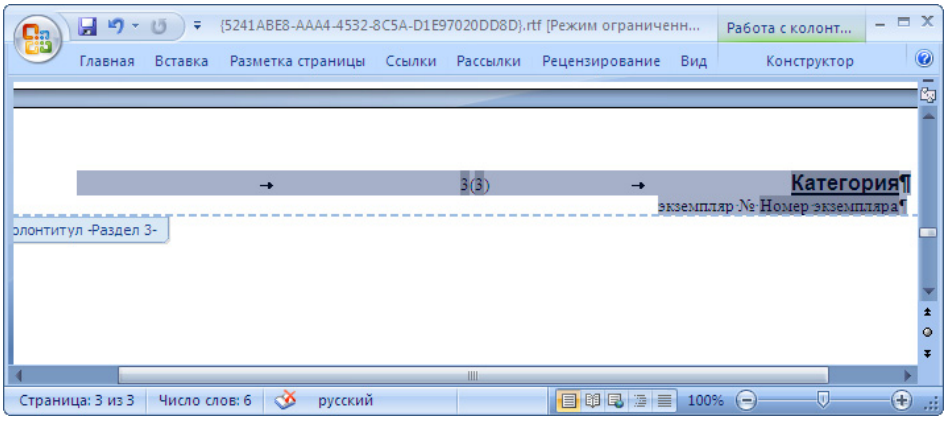
При удалении грифа из шаблона учитывайте следующую особенность: если шаблон содержит несколько грифов, необходимо удалить сам гриф, а затем разрыв раздела, которым удаленный гриф отделялся от других. То есть в шаблоне должно быть количество разрывов раздела (n–1), где n — количество грифов.

Для удаления грифа:

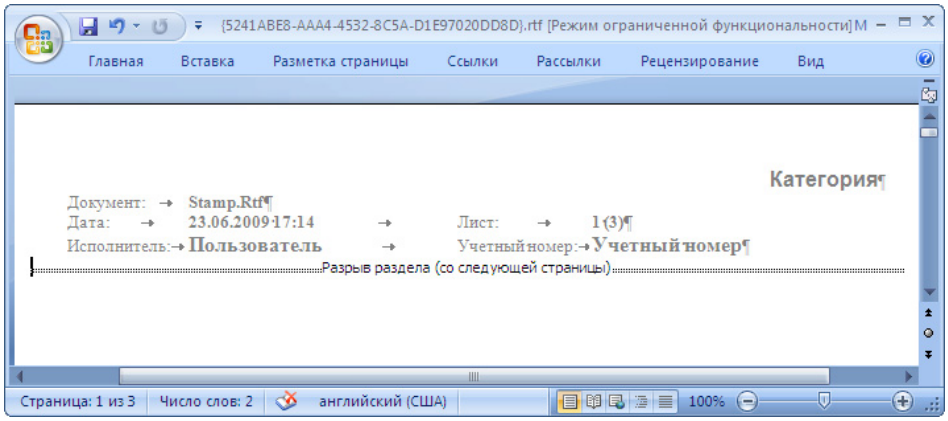
1. Вызовите файл шаблона для редактирования (см. стр. 14).
2. Перейдите к странице удаляемого грифа.
3. При наличии текста (полей) между верхним и нижним колонтитулами — выделите и удалите содержимое страницы.



4. При наличии текста (полей) в верхнем колонтитуле — откройте колонтитул, выделите и удалите содержимое колонтитула.



5. В текущем разделе включите оформление колонтитула предыдущего раздела. Для этого в зависимости от версии установленной программы MS Word выполните соответствующее действие:
   - в MS Word 2007 — на вкладке "Конструктор" в группе "Переходы" активируйте команду "Как в предыдущем разделе" и подтвердите удаление колонтитула текущего раздела в появившемся диалоге запроса;
   - в MS Word 2003 и более ранних версиях — в панели инструментов "Колонтитулы" нажмите кнопку "Как в предыдущем" и подтвердите удаление колонтитула текущего раздела в появившемся диалоге запроса.
6. Аналогичным образом удалите содержимое нижнего колонтитула (см. действия **4**–**5**).
7. Отключите режим редактирования колонтитулов. Для этого в зависимости от версии установленной программы MS Word выполните соответствующее действие:
   - в MS Word 2007 — на вкладке "Конструктор" в группе "Закрыть" активируйте команду "Закрыть окно колонтитулов";
   - в MS Word 2003 и более ранних версиях — в панели инструментов "Колонтитулы" нажмите кнопку "Закрыть".
8. Установите курсор в строке разрыва раздела.



9. Нажмите клавишу <Delete>.

Формирование содержимого грифа

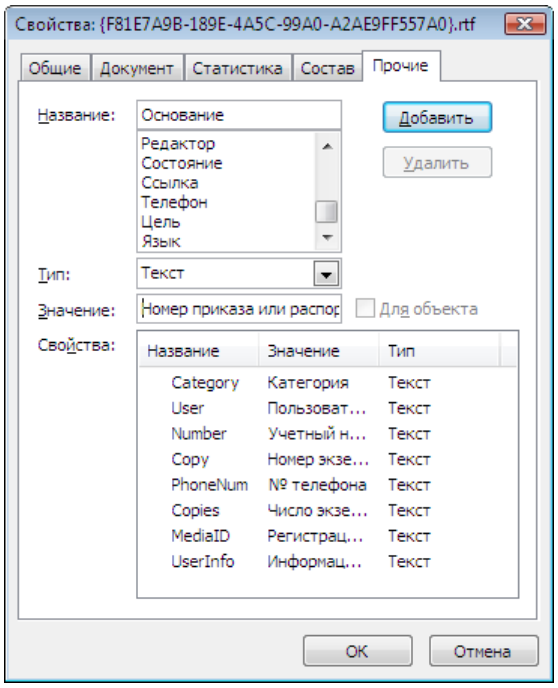
Содержимое грифа формируется с использованием стандартных средств и возможностей редактора MS Word.

В гриф можно добавлять как стандартные поля, относящиеся к свойствам документа и входящие в группу "DocProperty", так и нестандартные поля (т. е. отсутствующие в группе "DocProperty"). Чтобы добавить в гриф нестандартное поле, необходимо предварительно создать его в списке полей группы "DocProperty".

Для создания нестандартного поля:

1. Вызовите файл шаблона для редактирования (см. стр. 14).
2. Вызовите окно настройки свойств документа. Для этого в зависимости от версии установленной программы MS Word выполните соответствующее действие:
   - в MS Word 2007 — в верхнем левом углу окна программы нажмите кнопку "Office" и в открывшемся меню активируйте команду "Подготовить | Свойства";
   - в MS Word 2003 и более ранних версиях — в главном меню программы активируйте команду "Файл | Свойства".

3. В окне настройки свойств перейдите к диалогу "Прочие":



4. В поле "Название" введите краткое описание поля, раскрывающее его назначение.
5. В поле "Тип" выберите значение "Текст".
6. В поле "Значение" введите условное значение. Это значение будет отображаться в поле грифа. Само значение будет вводиться пользователем при выводе документа на печать.

> **Пример**. Требуется создать поле, где должно отображаться наименование документа (приказ, распоряжение), на основании которого выполняются какие-либо действия. Для поля можно указать название "Основание", а в качестве условного значения — "Номер приказа или распоряжения". При выводе конфиденциального документа на печать пользователь будет вводить по запросу вместо условного значения данные о соответствующем приказе или распоряжении.

7. Нажмите кнопку "Добавить" в верхней части диалога.

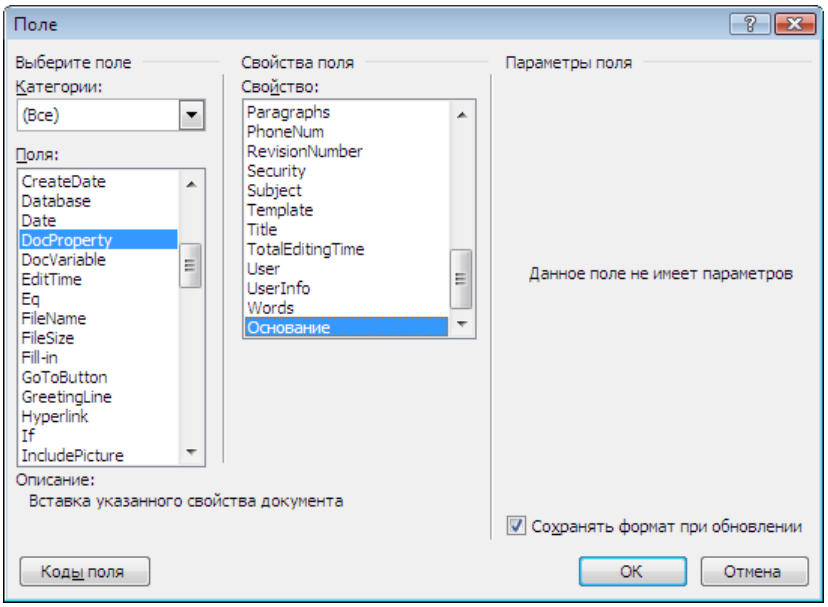
   Новое поле будет добавлено в список "Свойства".
8. Нажмите кнопку "OK" для закрытия диалога.

   Добавленное поле можно будет использовать при вставке полей в шаблон грифа (см. процедуру ниже).

Для добавления нестандартного поля в гриф:

1. Вызовите файл шаблона для редактирования (см. стр. 14).
2. Перейдите к нужному грифу и установите курсор в место предполагаемого размещения поля. Если поле должно размещаться в колонтитуле, предварительно следует открыть колонтитул.
3. Вызовите стандартный диалог MS Word "Поле". Для этого в зависимости от версии установленной программы MS Word выполните соответствующее действие:
   - в MS Word 2007 — перейдите на вкладку "Вставка" и в группе "Текст" активируйте команду "Экспресс-блоки | Поле";
   - в MS Word 2003 и более ранних версиях — в главном меню программы активируйте команду "Вставка | Поле".
4. В списке "Поля" выберите группу "DocProperty".

В диалоге появится список "Свойства поля":



Список содержит как стандартные поля MS Word, так и поля, добавленные средствами Secret Net 6 (в том числе нестандартные поля).

5. Выберите в списке "Свойства поля" название поля, предназначенного для вставки в гриф, и нажмите кнопку "OK".

   В грифе появится добавленное поле, отображающее заданное условное значение.

6. При необходимости добавьте в грифе пояснительный текст для поля.

Редактирование шаблона грифов для MS Excel

В шаблон грифов конфиденциальности для MS Excel можно включить не более трех грифов. Редактирование шаблона осуществляется в отдельных диалогах для каждого грифа.

Ввод в действие шаблона и загрузка для редактирования

Ввод в действие шаблона и загрузка грифов для редактирования осуществляется в оснастке для управления параметрами объектов групповой политики.

Для ввода в действие шаблона и редактирования грифов:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (описание процедуры вызова оснастки см. в документе [3]).
2. Выберите папку "Настройки подсистем".

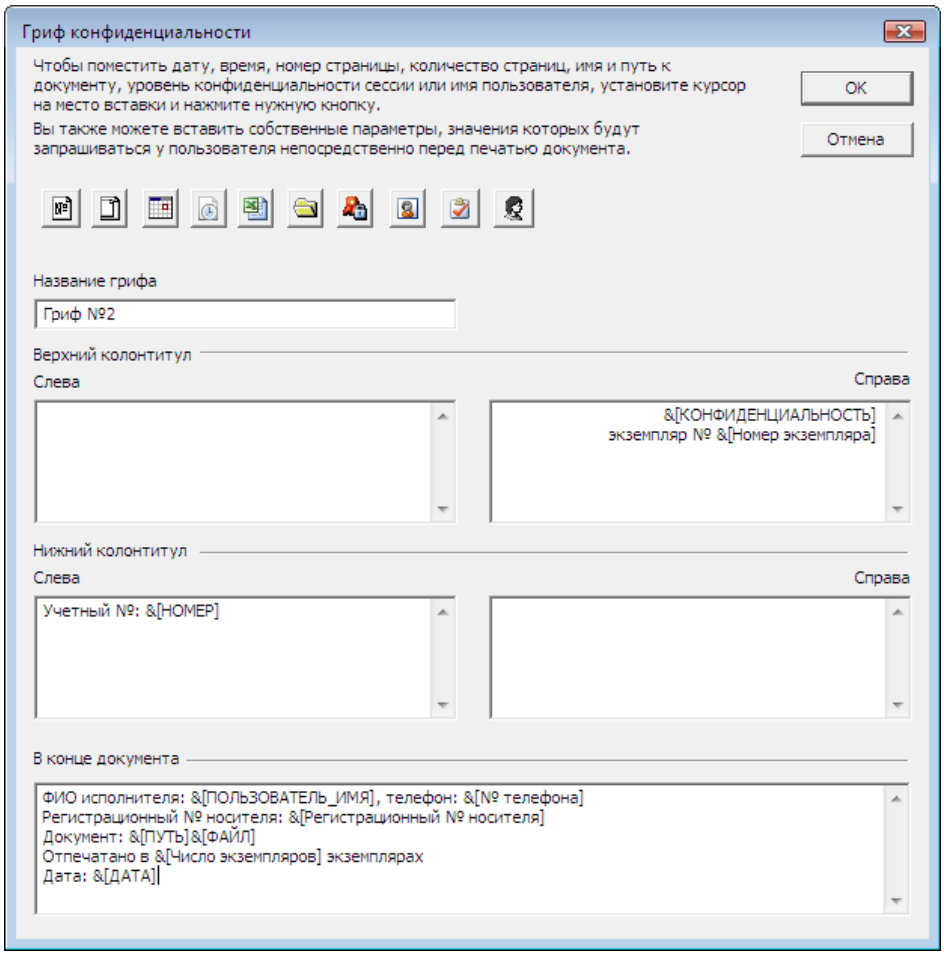
   В правой части окна появится список параметров.

3. Вызовите контекстное меню для параметра "Полномочное управление доступом: Гриф конфиденциальности для Microsoft Excel" и активируйте в нем команду "Свойства".

   На экране появится диалог настройки параметра.

4. Отметьте грифы, которые будут использоваться.
5. Чтобы отредактировать нужный гриф, нажмите кнопку "Изменить" рядом с названием грифа (кнопка активна, если напротив названия грифа установлена отметка).

На экране появится диалоговое окно для редактирования грифа.



6. Измените содержимое грифа (см. ниже) и нажмите кнопку "OK".
7. После редактирования грифов нажмите кнопку "OK" в диалоге настройки параметра.

Для ввода в действие шаблона по умолчанию:

1. Выполните действия **1**–**3** вышеописанной процедуры.
2. Нажмите кнопку "Вернуть исходные".
3. Нажмите кнопку "OK".

   Ранее заданный шаблон будет удален, и в систему будет загружен встроенный шаблон (используемый по умолчанию после установки системы Secret Net 6).

Формирование содержимого грифа

Содержимое грифа формируется в специальном диалоговом окне (см. выше).

В верхней части диалога расположены кнопки для вставки кодов полей (параметров) в гриф и поле для ввода названия грифа. В нижней части диалога расположены поля для ввода текста и кодов полей. Текст и коды полей можно указать для левой и правой областей колонтитулов (центральные области колонтитулов не используются), а также для последней страницы документа.

Для использования в грифе предусмотрены следующие коды полей:

- номер текущей страницы документа;
- количество страниц в документе;
- дата вывода документа на печать;
- время вывода на печать;
- имя файла;
- путь к файлу;

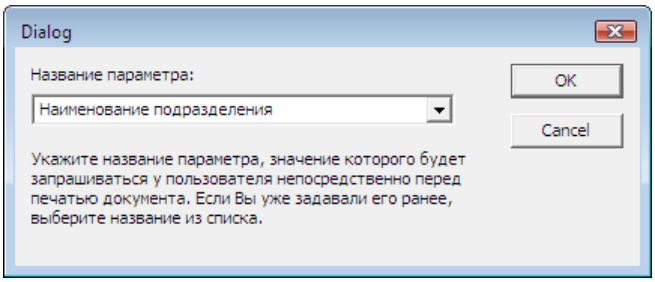
- категория конфиденциальности документа;
- имя пользователя, выполнившего печать;
- учетный номер документа (значение поля пользователь вводит при печати);
- "пользовательский параметр" — нестандартное добавленное поле (значение поля пользователь вводит при печати).

Для формирования содержимого грифа:

1. Вызовите диалоговое окно для редактирования грифа (см. выше).
2. Введите название грифа.
3. Чтобы изменить содержание левой области верхнего колонтитула, отредактируйте поле "Слева" в группе полей "Верхний колонтитул". Используйте стандартные операции редактирования текстовых полей. Добавление кодов полей можно выполнять вручную или с помощью кнопок в верхней части диалога.

4. Если требуется вставить нестандартный код поля, нажмите кнопку "Пользовательский параметр".

   На экране появится диалог:



5. Введите краткое описание поля (можно выбрать из списка одно из ранее использовавшихся значений) и нажмите кнопку "OK".
6. Аналогичным образом измените содержание других областей колонтитулов и последней страницы документа (см. действия **3**–**5**).
7. После внесения изменений нажмите кнопку "OK".

Приложение

Настройка работы механизма полномочного управления доступом

Для обеспечения корректности функционирования прикладных программ при использовании механизма полномочного управления доступом, а также для удобства работы администратора в системе Secret Net 6 реализованы некоторые дополнительные возможности настройки.

Перенаправление вывода общих служебных файлов

Механизм полномочного управления доступом выполняет проверку соответствия уровня допуска пользователя и категории конфиденциальности объекта доступа (каталог, файл). Однако в ряде приложений (например, MS Word) выполняется обращение к некоторым служебным файлам, при этом нет возможности изменять категорию их конфиденциальности, то есть данные сохраняются в одном и том же файле и каталоге, вне зависимости от уровня допуска пользователя. При использовании механизма полномочного управления доступом в режиме контроля потоков такие особенности приводят к конфликтным ситуациям и невозможности корректной работы приложений.

Для решения указанной проблемы в системе Secret Net 6 реализована функция перенаправления вывода общих служебных файлов, которым назначается соответствующая категория конфиденциальности. Функция действует в конфиденциальных и строго конфиденциальных сессиях. При обращении приложения к общему файлу драйвер полномочного управления доступом определяет пользователя, инициировавшего обращение, и уровень конфиденциальности его сессии. После этого драйвер, в соответствии с уровнем конфиденциальности сессии пользователя, организует чтение/запись информации в этот общий файл, но перенаправляет его в другой специальный каталог.

Для настройки данной функции в реестр операционной системы добавлен параметр HKLM\System\CurrentControlSet\Services\SNMC5xx\Params\SourceRedirect. В этом параметре хранится список путей к каталогам с общими файлами, для которых требуется создание дополнительных каталогов различной категории конфиденциальности. По умолчанию в этот список добавлены записи для каталогов, предназначенных для обслуживания обращений приложения MS Word:

ОС Windows 2000/XP/2003	ОС Windows Vista/2008/7
\Application Data\Microsoft\Templates	\AppData\Roaming\Microsoft\Templates
\Application Data\Microsoft\Шаблоны	\AppData\Roaming\Microsoft\Шаблоны

В зависимости от уровня конфиденциальности сессии пользователя, при обращении приложения к данным каталогам чтение/запись информации для общих файлов будет выполняться в одном из дополнительно созданных каталогов:

ОС Windows 2000/XP/2003	ОС Windows Vista/2008/7
\Application Data\Microsoft\Templates(1)	\AppData\Roaming\Microsoft\Templates(1)
\Application Data\Microsoft\Templates(2)	\AppData\Roaming\Microsoft\Templates(2)
\Application Data\Microsoft\Шаблоны(1)	\AppData\Roaming\Microsoft\Шаблоны(1)
\Application Data\Microsoft\Шаблоны(2)	\AppData\Roaming\Microsoft\Шаблоны(2)

При возникновении аналогичных конфликтных ситуаций с другими приложениями список путей к каталогам, для которых будет осуществляться перенаправление общих файлов, необходимо расширить.

При редактировании списка путей к каталогам ввод имен каталогов необходимо выполнять с учетом следующих особенностей:

- путь к каталогу может содержать как полный путь, однозначно определяющий данный каталог, так и его часть, позволяющую определить подмножество путей к каталогам. Если указывается подмножество путей, строка должна начинаться символом "\";
- путь к каталогу указывается БЕЗ символа "\" на конце;
- имена каталогов должны быть указаны в формате LFN — Long File Name.

Подавление регистрации событий для некоторых типов файлов

Данная настройка позволяет исключить регистрацию в журнале Secret Net событий, относящихся к внутрисистемным обращениям к файлам, сократив тем самым количество записей в журнале, которые анализирует администратор системы.

Для настройки драйвера в реестр операционной системы добавлен параметр HKLM\System\CurrentControlSet\Services\SNMC5xx\Params\EventSuppression. В этом параметре хранится список расширений файлов, регистрация событий с которыми в журнале не производится. Расширения записываются в виде ".lnk", ".tmp" и т. п. (можно указать любое расширение с помощью маски "*.*" или ".*"). По умолчанию список содержит файловое расширение ".lnk". При необходимости список можно дополнять с помощью штатных средств, позволяющих редактирование реестра ОС Windows.

Подавление сообщений о повышении категории конфиденциальности

При работе пользователя в конфиденциальной или строго конфиденциальной сессии всем создаваемым или редактируемым файлам присваивается категория конфиденциальности, соответствующая уровню сессии, в том числе и служебным файлам, которые, в частности, создаются приложением MS Word для корректного функционирования. Поскольку в этом случае категория конфиденциальности служебных файлов повышается, система защиты в соответствии с принятыми правилами должна выводить пользователю на экран сообщение об этом событии. С целью облегчения работы пользователя предусмотрены функции подавления вывода подобных сообщений для определенных типов служебных файлов (по расширению) и для файлов, находящихся в определенных каталогах.

Изменение списка расширений файлов

Системный реестр компьютера содержит дополнительный параметр HKLM\System\CurrentControlSet\Services\SNMC5xx\Params\MessageBoxSuppression. В этом параметре хранится список расширений файлов, для которых сообщение о повышении категории конфиденциальности не выводится на экран. Расширения указываются в виде ".tmp", ".lnk" и т. п. (можно указать любое расширение с помощью маски "*.*" или ".*"). По умолчанию список содержит расширения ".tmp", ".spl" и ".shd". При необходимости дополните список нужными расширениями с помощью программы редактирования реестра.

Изменение списка каталогов

Системный реестр компьютера содержит дополнительный параметр HKLM\System\CurrentControlSet\Services\SNMC5xx\Params\MessageBoxSuppressionByDir. Параметр хранит пути к каталогам с файлами, для которых сообщение о повышении категории конфиденциальности не выводится на экран вне зависимости от расширений файлов. По умолчанию список содержит записи:

ОС Windows 2000/XP/2003	ОС Windows Vista/2008/7
\Local Settings\Temp	\AppData\Local\Temp
\Local Settings\Temporary Internet Files\Content.MSO	\AppData\Local\Microsoft\Temporary Internet Files\Content.MSO
\Local Settings\Temporary Internet Files\Content.Word	\AppData\Local\Microsoft\Temporary Internet Files\Content.Word
\system32\spool\printers	\system32\spool\printers

При необходимости дополните список нужными каталогами с помощью программы редактирования реестра.

При редактировании списка путей ввод имен каталогов необходимо выполнять с учетом следующих особенностей:

- путь к каталогу может содержать как полный путь, однозначно определяющий данный каталог, так и его часть, позволяющую определить подмножество путей к каталогам. Если указывается подмножество путей, строка должна начинаться символом "\";
- путь к каталогу указывается БЕЗ символа "\" на конце;
- имена каталогов должны быть указаны в формате LFN.

Подавление сообщений о выводе конфиденциальной информации

При работе пользователя, имеющего привилегию "Вывод конфиденциальной информации", в конфиденциальной или строго конфиденциальной сессии он имеет право осуществлять отчуждение конфиденциального файла на внешний носитель информации. Поскольку в этом случае категория конфиденциальности отчуждаемого файла сбрасывается, система защиты в соответствии с принятыми правилами должна выводить пользователю на экран сообщение об этом событии. С целью облегчения работы пользователя предусмотрена функция подавления вывода подобных сообщений для определенных типов файлов (по расширению).

Изменение списка расширений файлов

В системный реестр компьютера можно включить дополнительный параметр HKLM\System\CurrentControlSet\Services\SNMC5xx\Params\MBS_SecretOutput. В этом параметре хранится список расширений файлов, для которых сообщение об отчуждении файла на внешний носитель не выводится на экран. Расширения указываются в виде ".tmp", ".lnk" и т. п. (можно указать любое расширение с помощью маски "*.*" или ".*"). По умолчанию параметр отсутствует в реестре. При необходимости его можно создать с помощью программы редактирования реестра, указав тип данных "Мультистроковый параметр". Затем список может быть наполнен нужными расширениями.

Документация

1	Средство защиты информации Secret Net 6. Принципы построения. Руководство администратора	RU.88338853.501410. 007 91 1
2	Средство защиты информации Secret Net 6. Установка, обновление и удаление. Руководство администратора	RU.88338853.501410. 007 91 2
3	Средство защиты информации Secret Net 6. Управление. Основные механизмы защиты. Руководство администратора	RU.88338853.501410. 007 91 3
4	Средство защиты информации Secret Net 6. Управление. Полномочное управление доступом и контроль печати. Руководство администратора	RU.88338853.501410. 007 91 4
5	Средство защиты информации Secret Net 6. Аудит. Руководство администратора	RU.88338853.501410. 007 91 5
6	Средство защиты информации Secret Net 6. Мониторинг и оперативное управление. Руководство администратора	RU.88338853.501410. 007 91 6
7	Средство защиты информации Secret Net 6. Конфигурирование. Руководство администратора	RU.88338853.501410. 007 91 7
8	Средство защиты информации Secret Net 6. Аппаратные средства. Руководство администратора	RU.88338853.501410. 007 91 8
9	Средство защиты информации Secret Net 6. Руководство пользователя	RU.88338853.501410. 007 92
10	Программно-аппаратный комплекс "Соболь". Версия 2.1. Руководство администратора	УВАЛ. 00300-58-01 91
11	Программно-аппаратный комплекс "Соболь". Версия 2.1. Руководство пользователя	УВАЛ. 00300-58-01 92
12	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора	RU.40308570.501410. 001 91
13	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство пользователя	RU.40308570.501410. 001 92

Предметный указатель